Singular numbers and Stickelberger relation

Roland Quême

2006 July 26

Contents

Abstract

Roland Quême
13 avenue du château d'eau
31490 Brax
France
tel : 0561067020
cel : 0684728729
mailto: roland.queme@wanadoo.fr
home page: http://roland.queme.free.fr/
****

V07 - MSC Classification : 11R18; 11R29
****

Let p be an odd prime. Let $K_p = \mathbb{Q}(\zeta_p)$ be the p-cyclotomic field and $\mathbb{Z}[\zeta_p]$ be the ring of integers of K_p. Let π be the prime ideal of K_p lying over p. Let G be the Galois group of K_p. Let v be a primitive root mod p. Let σ be a $\mathbb{Q}$-isomorphism of K_p defined by $\sigma : \zeta_p \to \zeta_p^v$. Let $P(\sigma) = \sigma^{p-2}v^{-(p-2)} + ... + \sigma v^{-1} + 1 \in \mathbb{Z}[G]$, where v^n is understood (mod p). Let C_p be the p-class group of K_p. Let $\mathbf{q}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ with $Cl(\mathbf{q}) \in C_p$. Let q the prime number lying above $\mathbf{q}$. Let A be a singular number defined by $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$. From Stickelberger relation we prove the π-adic congruences:

1. $\pi^{2p-1} \mid A^{P(\sigma)}$ if $q \equiv 1 \bmod p$,
2. $\pi^{2p-1} \parallel A^{P(\sigma)}$ if $q \equiv 1 \bmod p$ and $p^{(q-1)/p} \equiv 1(\bmod q)$.
3. $\pi^{2p} \mid A^{P(\sigma)}$ if $q \not\equiv 1 \bmod p$.

These results allow us to connect the structure of the p-class group C_p with π-adic expression of singular numbers A and with solutions of some explicit congruences mod p in $\mathbb{Z}[X]$. The last section connect Stickelberger relation with the class group $\mathbf{C}$ of K_p.

This paper is at elementary level in Classical Algebraic Number Theory.

1 Introduction

Let p be an odd prime. Let $\mathbf{F}_p$ be the finite field of p elements with no null part $\mathbf{F}_p^*$. Let $K_p = \mathbb{Q}(\zeta_p)$ be the p-cyclotomic field. Let π be the prime ideal of K_p lying over p. Let v be a primitive root mod p. For $n \in \mathbb{Z}$ let us note briefly v^n for $v^n \bmod p$. Let $\sigma : \zeta_p \to \zeta_p^v$ be a $\mathbb{Q}$-isomorphism of $K_p/\mathbb{Q}$. Let G_p be the Galois group of $K_p/\mathbb{Q}$. Let $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v^{-i}, \quad P(\sigma) \in \mathbb{Z}[G_p]$.

We suppose that p is an irregular prime. Let C_p be the p-class group of K_p. Let Γ be a subgroup of C_p of order p annihilated by $\sigma - \mu$ with $\mu \in \mathbf{F}_p^*$. From Kummer, there

exist not principal prime ideals $\mathbf{q}$ of $\mathbb{Z}[\zeta_p]$ of inertial degree 1 with class $Cl(\mathbf{q}) \in \Gamma$. Let q be the prime number lying above $\mathbf{q}$.

Let n be the smallest natural integer $1 < n \leq p-2$ such that $\mu \equiv v^n \bmod p$ for μ defined above. There exist singular numbers A with $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$ and $\pi^n \mid A - a^p$ where a is a natural number. If A is singular not primary then $\pi^n \parallel A - a^p$ and if A is singular primary then $\pi^p \mid A - a^p$. We prove, by an application of Stickelberger relation to the prime ideal $\mathbf{q}$, that now we can *climb* up to the π-adic congruence:

1. $\pi^{2p-1} \mid A^{P(\sigma)}$ if $q \equiv 1 \bmod p$.
2. $\pi^{2p-1} \parallel A^{P(\sigma)}$ if $q \equiv 1 \bmod p$ and $p^{(q-1)/p} \equiv 1 \bmod q$.
3. $\pi^{2p} \mid A^{P(\sigma)}$ if $q \not\equiv 1 \bmod p$.

This property of π-adic congruences on singular numbers is at the heart of this paper.

1. As a first example, in section 4 p. 15 this π-adic improvement allows us to find again an elementary straightforward proof that the relative p-class group C_p^- verifies the congruence

$$\sum_{i=1}^{p-2} v^{(2m+1)(i-1)} \times \left(\frac{v^{-(i-1)} - v^{-i} \times v}{p}\right) \equiv 0 \bmod p, \tag{1}$$

   for m taking r^- different integer values m_i, $\quad i = 1, \ldots, r^-$, $\quad 1 < m_i \leq \frac{p-3}{2}$ where r^- is the rank of the relative p-class group C_p^-.
2. The section 5 p. 19 connects the π-adic expansion of singular primary numbers with the structure of the p-class group of K_p.
3. In the section 6 p. 26 we give some explicit congruences derived of Stickelberger for prime ideals $\mathbf{q}$ of inertial degree $f > 1$.
4. Let $h(K_p)$ be the class number of K_p. In the last section 7 p. 28, we apply Stickelberger relation to describe structure of the complete class group $\mathbf{C}$ of K_p of order $h(K_p)$ (by opposite to previous sections applied to p-class group C_p) .

2 Some definitions

In this section we give the definitions and notations on cyclotomic fields, p-class group, singular numbers, primary and not primary,used in this paper.

1. Let p be an odd prime. Let ζ_p be a root of the polynomial equation $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$. Let K_p be the p-cyclotomic field $K_p = \mathbb{Q}(\zeta_p)$. The ring of integers of K_p is $\mathbb{Z}[\zeta_p]$. Let K_p^+ be the maximal totally real subfield of K_p. The ring of integers of K_p^+ is $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ with group of units $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$.

Let v be a primitive root $\bmod p$ and $\sigma : \zeta_p \to \zeta_p^v$ be a $\mathbb{Q}$-isomorphism of K_p. Let G_p be the Galois group of the extension $K_p/\mathbb{Q}$. Let $\mathbf{F}_p$ be the finite field of cardinal p with no null part $\mathbf{F}_p^*$. Let $\lambda = \zeta_p - 1$. The prime ideal of K_p lying over p is $\pi = \lambda\mathbb{Z}[\zeta_p]$.

2. Suppose that p is irregular. Let C_p be the p-class group of K_p. Let r be the rank of C_p. Let C_p^+ be the p-class group of K_p^+. Then $C_p = C_p^+ \oplus C_p^-$ where C_p^- is the relative p-class group.
3. Let Γ be a subgroup of order p of C_p annihilated by $\sigma - \mu \in \mathbf{F}_p[G_p]$ with $\mu \in \mathbf{F}_p^*$. Then $\mu \equiv v^n \bmod p$ with a natural integer n, $\quad 1 < n \leq p-2$.
4. An integer $A \in \mathbb{Z}[\zeta_p]$ is said singular if $A^{1/p} \notin K_p$ and if there exists an ideal $\mathbf{a}$ of $\mathbb{Z}[\zeta_p]$ such that $A\mathbb{Z}[\zeta_p] = \mathbf{a}^p$.
   (a) If $\Gamma \subset C_p^-$: then there exist singular integers A with $A\mathbb{Z}[\zeta_p] = \mathbf{a}^p$ where $\mathbf{a}$ is a **not** principal ideal of $\mathbb{Z}[\zeta_p]$ verifying simultaneously

$$\begin{aligned} &Cl(\mathbf{a}) \in \Gamma, \\ &\sigma(A) = A^\mu \times \alpha^p, \quad \mu \in \mathbf{F}_p^*, \quad \alpha \in K_p, \\ &\mu \equiv v^{2m+1} \bmod p, \quad m \in \mathbb{N}, \quad 1 \leq m \leq \frac{p-3}{2}, \\ &\pi^{2m+1} \mid A - a^p, \quad a \in \mathbb{N}, \quad 1 \leq a \leq p-1, \end{aligned} \tag{2}$$

   Moreover, this number A verifies

$$A \times \overline{A} = D^p, \tag{3}$$

   for some integer $D \in O_{K_p^+}$.
      i. This integer A is singular not primary if $\pi^{2m+1} \parallel A - a^p$.
      ii. This integer A is singular primary if $\pi^p \mid A - a^p$.
   (b) If $\Gamma \subset C_p^+$: then there exist singular integers A with $A\mathbb{Z}[\zeta_p] = \mathbf{a}^p$ where $\mathbf{a}$ is a **not** principal ideal of $\mathbb{Z}[\zeta_p]$ verifying simultaneously

$$\begin{aligned} &Cl(\mathbf{a}) \in \Gamma, \\ &\sigma(A) = A^\mu \times \alpha^p, \quad \mu \in \mathbf{F}_p^*, \quad \alpha \in K_p, \\ &\mu \equiv v^{2m} \bmod p, \quad m \in \mathbb{Z}, \quad 1 \leq m \leq \frac{p-3}{2}, \\ &\pi^{2m} \mid A - a^p, \quad a \in \mathbb{Z}, \quad 1 \leq a \leq p-1, \end{aligned} \tag{4}$$

   Moreover, this number A verifies

$$\frac{A}{\overline{A}} = D^p, \tag{5}$$

   for some number $D \in K_p^+$.

i. This integer A is singular not primary if $\pi^{2m} \parallel A - a^p$.

ii. This number A is singular primary if $\pi^p \mid A - a^p$.

3 On Kummer and Stickelberger relation

1. Let $q \neq p$ be an odd prime. Let ζ_q be a root of the minimal polynomial equation $X^{q-1} + X^{q-2} + \cdots + X + 1 = 0$. Let $K_q = \mathbb{Q}(\zeta_q)$ be the q-cyclotomic field. The ring of integers of K_q is $\mathbb{Z}[\zeta_q]$. Here we fix a notation for the sequel. Let u be a primitive root $\mod q$. For every integer $k \in \mathbb{Z}$ then u^k is understood $\mod q$ so $1 \leq u^k \leq q-1$. If $k < 0$ it is to be understood as $u^k u^{-k} \equiv 1 \mod q$. Let $K_{pq} = \mathbb{Q}(\zeta_p, \zeta_q)$. Then K_{pq} is the compositum $K_p K_q$. The ring of integers of K_{pq} is $\mathbb{Z}[\zeta_{pq}]$.

2. Let $\mathbf{q}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ lying over the prime q. Let $m = N_{K_p/\mathbb{Q}}(\mathbf{q}) = q^f$ where f is the smallest integer such that $q^f \equiv 1 \mod p$. If $\psi(\alpha) = a$ is the image of $\alpha \in \mathbb{Z}[\zeta_p]$ under the natural map $\psi : \mathbb{Z}[\zeta_p] \to \mathbb{Z}[\zeta_p]/\mathbf{q}$, then for $\psi(\alpha) = a \not\equiv 0$ define a character $\chi_{\mathbf{q}}^{(p)}$ on $\mathbf{F}_m = \mathbb{Z}[\zeta_p]/\mathbf{q}$ by

$$\chi_{\mathbf{q}}^{(p)}(a) = \{\frac{\alpha}{\mathbf{q}}\}_p^{-1} = \overline{\{\frac{\alpha}{\mathbf{q}}\}}_p, \tag{6}$$

where $\{\frac{\alpha}{\mathbf{q}}\} = \zeta_p^c$ for some natural integer c, is the p^{th} power residue character $\mod \mathbf{q}$. We define

$$g(\mathbf{q}) = \sum_{x \in \mathbf{F}_m} (\chi_{\mathbf{q}}^{(p)}(x) \times \zeta_q^{Tr_{\mathbf{F}_m/\mathbf{F}_q}(x)}) \in \mathbb{Z}[\zeta_{pq}], \tag{7}$$

and $\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p$. It follows that $\mathbf{G}(\mathbf{q}) \in \mathbb{Z}[\zeta_{pq}]$. Moreover $\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p \in \mathbb{Z}[\zeta_p]$, see for instance Mollin [6] prop. 5.88 (c) p. 308.

The Stickelberger's relation is classically:

Theorem 3.1. *In $\mathbb{Z}[\zeta_p]$ we have the ideal decomposition*

$$\mathbf{G}(\mathbf{q})\mathbb{Z}[\zeta_p] = \mathbf{q}^S, \tag{8}$$

with $S = \sum_{t=1}^{p-1} t \times \varpi_t^{-1}$ where $\varpi_t \in Gal(K_p/\mathbb{Q})$ is given by $\varpi_t : \zeta_p \to \zeta_p^t$.

See for instance Mollin [6] thm. 5.109 p. 315.

3.1 On the structure of G(q).

In this subsection we are studying carefully the structure of $g(\mathbf{q})$ and $\mathbf{G}(\mathbf{q})$.

Lemma 3.2. *If $q \not\equiv 1$ mod p then $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.*

Proof.

1. Let u be a primitive root mod q. Let $\tau : \zeta_q \to \zeta_q^u$ be a $\mathbb{Q}$-isomorphism generating $Gal(K_q/\mathbb{Q})$. The isomorphism τ is extended to a K_p-isomorphism of K_{pq} by $\tau : \zeta_q \to \zeta_q^u, \quad \zeta_p \to \zeta_p$. Then $g(\mathbf{q})^p = \mathbf{G}(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ and so

$$\tau(g(\mathbf{q}))^p = g(\mathbf{q})^p,$$

and it follows that there exists a natural integer ρ with $\rho < p$ such that

$$\tau(g(\mathbf{q})) = \zeta_p^\rho \times g(\mathbf{q}).$$

Then $N_{K_{pq}/K_p}(\tau(g(\mathbf{q}))) = \zeta_p^{(q-1)\rho} \times N_{K_{pq}/K_p}(g(\mathbf{q}))$ and so $\zeta_p^{\rho(q-1)} = 1$.

2. If $q \not\equiv 1 \bmod p$, it implies that $\zeta_p^\rho = 1$ and so that $\tau(g(\mathbf{q})) = g(\mathbf{q})$ and thus that $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.

□

Let us note in the sequel $g(\mathbf{q}) = \sum_{i=0}^{q-2} g_i \times \zeta_q^i$ with $g_i \in \mathbb{Z}[\zeta_p]$.

Lemma 3.3. *If $q \equiv 1$ mod p then $g_0 = 0$.*

Proof. Suppose that $g_0 \neq 0$ and search for a contradiction: we start of

$$\tau(g(\mathbf{q})) = \zeta_p^\rho \times g(\mathbf{q}).$$

We have $g(\mathbf{q}) = \sum_{i=0}^{q-2} g_i \times \zeta_q^i$ and so $\tau(g(\mathbf{q})) = \sum_{i=0}^{q-2} g_i \times \zeta_q^{iu}$, therefore

$$\sum_{i=0}^{q-2} (\zeta_p^\rho \times g_i) \times \zeta_q^i = \sum_{i=0}^{q-2} g_i \times \zeta_q^{iu},$$

thus $g_0 = \zeta_p^\rho \times g_0$ and so $\zeta_p^\rho = 1$ which implies that $\tau(g(\mathbf{q})) = g(\mathbf{q})$ and so $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$. Then $\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p$ and so Stickelberger relation leads to $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^S$ where $S = \sum_{t=1}^{p-1} t \times \varpi_t^{-1}$. Therefore $\varpi_1^{-1}(\mathbf{q}) \parallel \mathbf{q}^S$ because q splits totally in $K_p/\mathbb{Q}$ and $\varpi_t^{-1}(\mathbf{q}) \neq \varpi_{t'}^{-1}(\mathbf{q})$ for $t \neq t'$. This case is not possible because the first member $g(\mathbf{q})^p$ is a p-power. □

Here we give an elementary computation of $g(\mathbf{q})$ not involving directly the Gauss Sums.

Lemma 3.4. *If $q \equiv 1$ mod p then*

$$
\begin{aligned}
&\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p, \\
&g(\mathbf{q}) = \zeta_q + \zeta_p^{\rho}\zeta_q^{u^{-1}} + \zeta_p^{2\rho}\zeta_q^{u^{-2}} + \cdots + \zeta_p^{(q-2)\rho}\zeta_q^{u^{-(q-2)}}, \\
&g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^S,
\end{aligned} \tag{9}
$$

for some natural number $\rho, \quad 1 < \rho \leq p-1$.

Proof.

1. We start of $\tau(g(\mathbf{q})) = \zeta_p^{\rho} \times g(\mathbf{q})$ and so

$$\sum_{i=1}^{q-2} g_i\zeta_q^{ui} = \zeta_p^{\rho} \times \sum_{i=1}^{q-2} g_i\zeta_q^{i}, \tag{10}$$

   which implies that $g_i = g_1\zeta_p^{\rho}$ for $u \times i \equiv 1$ mod q and so $g_{u^{-1}} = g_1\zeta_p^{\rho}$ (where u^{-1} is to be understood by u^{-1} mod q, so $1 \leq u^{-1} \leq q-1$).

2. Then $\tau^2(g(\mathbf{q})) = \tau(\zeta_p^{\rho}g(\mathbf{q})) = \zeta_p^{2\rho}g(\mathbf{q})$. Then

$$\sum_{i=1}^{q-2} g_i\zeta_q^{u^2 i} = \zeta_p^{2\rho} \times (\sum_{i=1}^{q-2} g_i\zeta_q^{i}),$$

   which implies that $g_i = g_1\zeta_p^{2\rho}$ for $u^2 \times i \equiv 1$ mod q and so $g_{u^{-2}} = g_1\zeta_p^{2\rho}$.

3. We continue up to $\tau^{(q-2)\rho}(g(\mathbf{q})) = \tau^{q-3}(\zeta_p^{\rho}g(\mathbf{q})) = \cdots = \zeta_p^{(q-2)\rho}g(\mathbf{q})$. Then

$$\sum_{i=1}^{q-2} g_i\zeta_q^{u^{q-2} i} = \zeta_p^{(q-2)\rho} \times (\sum_{i=1}^{q-2} g_i\zeta_q^{i}),$$

   which implies that $g_i = g_1\zeta_p^{(q-2)\rho}$ for $u^{q-2} \times i \equiv 1$ mod q and so $g_{u^{-(q-2)}} = g_1\zeta_p^{(q-2)\rho}$.

4. Observe that u is a primitive root mod q and so u^{-1} is a primitive root mod q. Then it follows that $g(\mathbf{q}) = g_1 \times (\zeta_q + \zeta_p^{\rho}\zeta_q^{u^{-1}} + \zeta_p^{2\rho}\zeta_q^{u^{-2}} + \ldots \zeta_p^{(q-2)\rho}\zeta_q^{u^{-(q-2)}})$. Let $U = \zeta_q + \zeta_p^{\rho}\zeta_q^{u^{-1}} + \zeta_p^{2\rho}\zeta_q^{u^{-2}} + \ldots \zeta_p^{(q-2)\rho}\zeta_q^{u^{-(q-2)}}$.

5. We prove now that $g_1 \in \mathbb{Z}[\zeta_p]^*$. From Stickelberger relation $g_1^p \times U^p = \mathbf{q}^S$. From $S = \sum_{i=1}^{p-1} \varpi_t^{-1} \times t$ it follows that $\varpi_t^{-1}(\mathbf{q})^t \parallel \mathbf{q}^S$ and so that $g_1 \not\equiv 0$ mod $\varpi_t^{-1}(\mathbf{q})$ because g_1^p is a p-power, which implies that $g_1 \in \mathbb{Z}[\zeta_p]^*$. Let us consider the relation(7). Let $x = 1 \in \mathbf{F}_q$, then $Tr_{\mathbf{F}_q/\mathbf{F}_q}(x) = 1$ and $\chi_{\mathbf{q}}^{(p)}(1) = 1^{(q-1)/p}$ mod $\mathbf{q} = 1$ and thus the coefficient of ζ_q is 1 and so $g_1 = 1$.

6. From Stickelberger, $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^S$, which achieves the proof.

□

Remark: From

$$
\begin{aligned}
& g(\mathbf{q}) = \zeta_q + \zeta_p^{\rho}\zeta_q^{u^{-1}} + \zeta_p^{2\rho}\zeta_q^{u^{-2}} + \cdots + \zeta_p^{(q-2)\rho}\zeta_q^{u^{-(q-2)}}, \\
(11) \qquad & \Rightarrow \tau(g(\mathbf{q})) = \zeta_q^{u} + \zeta_p^{\rho}\zeta_q + \zeta_p^{2\rho}\zeta_q^{u^{-1}} + \cdots + \zeta_p^{(q-2)\rho}\zeta_q^{u^{-(q-3)}}, \\
& \Rightarrow \zeta^{\rho} \times g(\mathbf{q}) = \zeta^{\rho}\zeta_q + \zeta_p^{2\rho}\zeta_q^{u^{-1}} + \zeta_p^{3\rho}\zeta_q^{u^{-2}} + \cdots + \zeta_p^{(q-1)\rho}\zeta_q^{u^{-(q-2)}}
\end{aligned}
$$

and we can verify directly that $\tau(g(\mathbf{q})) = \zeta_p^{\rho} \times g(\mathbf{q})$ for this expression of $g(\mathbf{q})$, observing that $q - 1 \equiv 0 \bmod p$.

Lemma 3.5. *Let $S = \sum_{t=1}^{p-1} \varpi_t^{-1} \times t$ where ϖ_t is the $\mathbb{Q}$-isomorphism given by $\varpi_t : \zeta_p \to \zeta_p^t$ of K_p. Let v be a primitive root mod p. Let σ be the $\mathbb{Q}$-isomorphism of K_p given by $\zeta_p \to \zeta_p^v$. Let $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v^{-i} \in \mathbb{Z}[G_p]$. Then $S = P(\sigma)$.*

Proof. Let us consider one term $\varpi_t^{-1} \times t$. Then $v^{-1} = v^{p-2}$ is a primitive root mod p because $p-2$ and $p-1$ are coprime and so there exists one and one i such that $t = v^{-i}$. Then $\varpi_{v^{-i}} : \zeta_p \to \zeta_p^{v^{-i}}$ and so $\varpi_{v^{-i}}^{-1} : \zeta_p \to \zeta_p^{v^i}$ and so $\varpi_{v^{-i}}^{-1} = \sigma^i$ (observe that $\sigma^{p-1} \times v^{-(p-1)} = 1$), which achieves the proof. □

Remark : The previous lemma is a verification of the consistency of classical results for instance in Ribenboim [9] p. 118, of Mollin [6] p. 315 and of Ireland-Rosen p. 209 with our computation. In the sequel we use Ribenboim notation more adequate for the factorization in $\mathbf{F}_p[G]$. When $q \equiv 1 \bmod p$ the Stickelberger's relation is connected with the Kummer's relation on Jacobi resolvents, see for instance Ribenboim, [9] (2A) b. p. 118 and (2C) relation (2.6) p. 119.

Lemma 3.6. *If $q \equiv 1$ mod p then*

1. *$g(\mathbf{q})$ defined in relation (9) is the Jacobi resolvent: $g(\mathbf{q}) =< \zeta_p^{-v}, \zeta_q >$.*

Proof.

1. $g(\mathbf{q}) =< \zeta_p^{-v}, \zeta_q >$: apply formula of Ribenboim [9] (2.2) p. 118 with $p = p, q = q, \zeta = \zeta_p, \quad \rho = \zeta_q, \quad n = \rho, \quad u = i, \quad m = 1$ and $h = u^{-1}$ (where the left members notations $p, q, \zeta, \rho, n, u, m$ and h are the Ribenboim notations).
2. We start of $< \zeta_p^{\rho}, \zeta_q >= g(\mathbf{q})$. Then v is a primitive root mod p, so there exists a natural integer l such that $\rho \equiv v^l \bmod p$. By conjugation σ^{-l} we get $< \zeta_p, \zeta_q >= g(\mathbf{q})^{\sigma^{-l}}$. Raising to p-power $< \zeta_p, \zeta_q >^p = g(\mathbf{q})^{p\sigma^{-l}}$. From lemma 3.5 and Stickelberger relation $< \zeta_p, \zeta_q >^p \mathbb{Z}[\zeta_p] = \mathbf{q}^{P(\sigma)\sigma^{-l}}$. From Kummer's relation (2.6) p. 119 in Ribenboim [9], we get $< \zeta_p, \zeta_q >^p \mathbb{Z}[\zeta_p] = \mathbf{q}^{P_1(\sigma)}$ with $P_1(\sigma) = \sum_{j=0}^{p-2} \sigma^j v^{(p-1)/2-j}$. Therefore $\sum_{i=0}^{p-2} \sigma^{i-l} v^{-i} = \sum_{j=0}^{p-2} \sigma^j v^{(p-1)/2-j}$. Then $i - l \equiv j \bmod p$ and $-i \equiv \frac{p-1}{2} - j \bmod p$ (or $i \equiv j - \frac{p-1}{2} \bmod p$) imply that

$j - \frac{p-1}{2} - l \equiv j \bmod p$, so $l + \frac{p-1}{2} \equiv 0 \bmod p$, so $l \equiv -\frac{p-1}{2} \bmod p$, and $l \equiv \frac{p+1}{2} \bmod p$, thus $\rho \equiv v^{(p+1)/2} \bmod p$ and finally $\rho = -v$.

□

Remark : The previous lemma allows to verify the consistency of our computation with Jacobi resultents used in Kummer (see Ribenboim p. 118-119).

Lemma 3.7. *If* $\mathbf{q} \equiv 1$ *mod* p *then* $g(\mathbf{q}) \equiv -1$ *mod* π.

Proof. From $g(\mathbf{q}) = \zeta_q + \zeta_p^{-v}\zeta_q^{u^{-1}} + \zeta_p^{-2v}\zeta_q^{u^{-2}} + \cdots + \zeta_p^{-(q-2)v}\zeta_q^{u^{-(q-2)}}$, we see that $g(\mathbf{q}) \equiv \zeta_q + \zeta_q^{u^{-1}} + \zeta_q^{u^{-2}} + \cdots + \zeta_q^{u^{-(q-2)}} \bmod \pi$. From u^{-1} primitive root $\bmod p$ it follows that $1 + \zeta_q + \zeta_q^{u^{-1}} + \zeta_q^{u^{-2}} + \cdots + \zeta_q^{u^{-(q-2)}} = 0$, which leads to the result. □

It is possible to improve the previous result to:

Lemma 3.8. *Suppose that* $q \equiv 1$ *mod* p. *If* $p^{(q-1)/p} \not\equiv 1$ *mod* q *then* $\pi^p \parallel g(\mathbf{q})^p + 1$.

Proof.

1. We start of $g(\mathbf{q}) = \zeta_q + \zeta_p^{\rho}\zeta_q^{u^{-1}} + \zeta_p^{2\rho}\zeta_q^{u^{-2}} + \ldots \zeta_p^{(q-2)\rho}\zeta_q^{u^{-(q-2)}}$ with $\rho = -v$, so

   $g(\mathbf{q}) = \zeta_q + ((\zeta_p^{\rho} - 1) + 1)\zeta_q^{u^{-1}} + ((\zeta_p^{2\rho} - 1) + 1)\zeta_q^{u^{-2}}, + \ldots ((\zeta_p^{(q-2)\rho} - 1) + 1)\zeta_q^{u^{-(q-2)}}$

   also

   $$g(\mathbf{q}) = -1 + (\zeta_p^{\rho} - 1)\zeta_q^{u^{-1}} + (\zeta_p^{2\rho} - 1)\zeta_q^{u^{-2}} + \cdots + (\zeta_p^{(q-2)\rho} - 1)\zeta_q^{u^{-(q-2)}}.$$

   Then $\zeta_p^{i\rho} \equiv 1 + i\rho\lambda \bmod \pi^2$, so

   $$g(\mathbf{q}) \equiv -1 + \lambda \times (\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \cdots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}) \bmod \lambda^2.$$

   Then $g(\mathbf{q}) = -1 + \lambda U + \lambda^2 V$ with $U = \rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \cdots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}$ and $U, V \in \mathbb{Z}[\zeta_{pq}]$.
2. Suppose that $\pi^{p+1} \mid g(\mathbf{q})^p + 1$ and search for a contradiction: then, from $g(\mathbf{q})^p = (-1 + \lambda U + \lambda^2 V)^p$, it follows that $p\lambda U + \lambda^p U^p \equiv 0 \bmod \pi^{p+1}$ and so $U^p - U \equiv 0 \bmod \pi$ because $p\lambda + \lambda^p \equiv 0 \bmod \pi^{p+1}$. Therefore

   $$\begin{aligned}&(\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \cdots + (q-2)\rho)\zeta_q^{u^{-(q-2)}})^p - \\ &(\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \cdots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}) \equiv 0 \bmod \lambda,\end{aligned}$$

   and so

   $$\begin{aligned}&(\rho\zeta_q^{pu^{-1}} + 2\rho\zeta_q^{pu^{-2}} + \cdots + (q-2)\rho)\zeta_q^{pu^{-(q-2)}}) \\ &- (\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \cdots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}) \equiv 0 \bmod \lambda.\end{aligned}$$

3. For any natural j with $1 \leq j \leq q-2$, there must exist a natural j' with $1 \leq j' \leq q-2$ such that simultaneously:

$$pu^{-j'} \equiv u^{-j} \bmod q \Rightarrow p \equiv u^{j'-j} \bmod q,$$
$$\rho j' \equiv \rho j \bmod \pi \Rightarrow j' - j \equiv 0 \bmod p.$$

Therefore $p \equiv u^{p \times \{(j'-j)/p\}} \bmod q$ and so $p^{(q-1)/p} \equiv u^{p \times (q-1)/p) \times \{(j'-j)/p\}} \bmod q$ thus $p^{(q-1)/p} \equiv 1 \bmod q$, contradiction.

□

3.2 A study of polynomial $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i v^{-i}$ of $\mathbb{Z}[G_p]$.

Recall that $P(\sigma) \in \mathbb{Z}[G_p]$ has been defined by $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i v^{-i}$.

Lemma 3.9.

$$P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v^{-i} = v^{-(p-2)} \times \{ \prod_{k=0,\ k \neq 1}^{p-2} (\sigma - v^k)\} + p \times R(\sigma), \tag{12}$$

where $R(\sigma) \in \mathbb{Z}[G_p]$ *with* $deg(R(\sigma)) < p-2$.

Proof. Let us consider the polynomial $R_0(\sigma) = P(\sigma) - v^{-(p-2)} \times \{\prod_{k=0,\ k \neq 1}^{p-2} (\sigma - v^k)\}$ in $\mathbf{F}_p[G_p]$. Then $R_0(\sigma)$ is of degree smaller than $p-2$ and the two polynomials $\sum_{i=0}^{p-2} \sigma^i v^{-i}$ and $\prod_{k=0,\ k \neq 1}^{p-2} (\sigma - v^k)$ take a null value in $\mathbf{F}_p[G_p]$ when σ takes the $p-2$ different values $\sigma = v^k$ for $k = 0, \ldots, p-2, \quad k \neq 1$. Then $R_0(\sigma) = 0$ in $\mathbf{F}_p[G_p]$ which leads to the result in $\mathbb{Z}[G_p]$. □

Let us note in the sequel

$$T(\sigma) = v^{-(p-2)} \times \prod_{k=0,\ k \neq 1}^{p-2} (\sigma - v^k). \tag{13}$$

Lemma 3.10.

$$P(\sigma) \times (\sigma - v) = T(\sigma) \times (\sigma - v) + pR(\sigma) \times (\sigma - v) = p \times Q(\sigma), \tag{14}$$

where $Q(\sigma) = \sum_{i=1}^{p-2} \delta_i \times \sigma^i \in \mathbb{Z}[G_p]$ *is given by*

$$
\begin{aligned}
\delta_{p-2} &= \frac{v^{-(p-3)} - v^{-(p-2)}v}{p}, \\
\delta_{p-3} &= \frac{v^{-(p-4)} - v^{-(p-3)}v}{p}, \\
&\vdots \\
\delta_i &= \frac{v^{-(i-1)} - v^{-i}v}{p}, \\
&\vdots \\
\delta_1 &= \frac{1 - v^{-1}v}{p},
\end{aligned}
\tag{15}
$$

with $-p < \delta_i \leq 0$.

Proof. We start of the relation in $\mathbb{Z}[G_p]$

$$P(\sigma) \times (\sigma - v) = v^{-(p-2)} \times \prod_{k=0}^{p-2}(\sigma - v^k) + p \times R(\sigma) \times (\sigma - v) = p \times Q(\sigma),$$

with $Q(\sigma) \in \mathbb{Z}[G_p]$ because $\prod_{k=0}^{p-2}(\sigma - v^k) = 0$ in $\mathbf{F}_p[G_p]$ and so $\prod_{k=0}^{p-2}(\sigma - v^k) = p \times R_1(\sigma)$ in $\mathbb{Z}[G_p]$. Then we identify in $\mathbb{Z}[G_p]$ the coefficients in the relation

$$
\begin{aligned}
&(v^{-(p-2)}\sigma^{p-2} + v^{-(p-3)}\sigma^{p-3} + \cdots + v^{-1}\sigma + 1) \times (\sigma - v) = \\
&p \times (\delta_{p-2}\sigma^{p-2} + \delta_{p-3}\sigma^{p-3} + \cdots + \delta_1\sigma + \delta_0),
\end{aligned}
$$

where $\sigma^{p-1} = 1$. □

Remark:

1. Observe that, with our notations, $\delta_i \in \mathbb{Z}, \quad i = 1, \ldots, p-2$, but generally $\delta_i \not\equiv 0 \bmod p$.
2. We see also that $-p < \delta_i \leq 0$. Observe also that $\delta_0 = \frac{v^{-(p-2)} - v}{p} = 0$.

Lemma 3.11. *The polynomial* $Q(\sigma)$ *verifies*

$$Q(\sigma) = \{(1-\sigma)(\sum_{i=0}^{(p-3)/2} \delta_i \times \sigma^i) + (1-v)\sigma^{(p-1)/2}\} \times (\sum_{i=0}^{(p-3)/2} \sigma^i). \tag{16}$$

Proof. We start of $\delta_i = \frac{v^{-(i-1)} - v^{-i}v}{p}$. Then

$$\delta_{i+(p-1)/2} = \frac{v^{-(i+(p-1)/2-1)} - v^{-(i+(p-1)/2)}}{p} = \frac{p - v^{-(i-1)} - (p - v^{-i})v}{p} = 1 - v - \delta_i.$$

Then

$$\begin{aligned} Q(\sigma) &= \sum_{i=0}^{(p-3)/2} (\delta_i \times (\sigma^i - \sigma^{i+(p-1)/2} + (1-v)\sigma^{i+(p-1)/2}) \\ &= (\sum_{i=0}^{(p-3)/2} \delta_i \times \sigma^i) \times (1 - \sigma^{(p-1)/2}) + (1-v) \times \sigma^{(p-1)/2} \times (\sum_{i=0}^{(p-3)/2} \sigma^i), \end{aligned}$$

which leads to the result. □

3.3 π-adic congruences on the singular integers A

From now we suppose that the prime ideal $\mathbf{q}$ of $\mathbb{Z}[\zeta_p]$ has a class $Cl(\mathbf{q}) \in \Gamma$ where Γ is a subgroup of order p of C_p previously defined, with a singular integer A given by $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$.

In an other part, we know that the group of ideal classes of the cyclotomic field is generated by the ideal classes of prime ideals of degree 1, see for instance Ribenboim, [9] (3A) p. 119.

Lemma 3.12.
$(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} = (\frac{A}{\overline{A}})^{P(\sigma)}$.

Proof. We start of $\mathbf{G}(\mathbf{q})\mathbb{Z}[\zeta_p] = g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^S$. Raising to p-power we get $g(\mathbf{q})^{p^2}\mathbb{Z}[\zeta_p] = \mathbf{q}^{pS}$. But $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$, so

$$g(\mathbf{q})^{p^2}\mathbb{Z}[\zeta_p] = A^S\mathbb{Z}[\zeta_p], \tag{17}$$

so

$$g(\mathbf{q})^{p^2} \times \zeta_p^w \times \eta = A^S, \quad \eta \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*, \tag{18}$$

where w is a natural number. Therefore, by complex conjugation, we get $\overline{g(\mathbf{q})}^{p^2} \times \zeta_p^{-w} \times \eta = \overline{A}^S$. Then $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} \times \zeta_p^{2w} = (\frac{A}{\overline{A}})^S$. From $A \equiv a \bmod \pi^m$ with a, m natural integers, $2 \leq m \leq p-1$, we get $\frac{A}{\overline{A}} \equiv 1 \bmod \pi^m$ and so $w = 0$. Then $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} = (\frac{A}{\overline{A}})^S$. □

Remark: Observe that this lemma is true if either $q \equiv 1 \bmod p$ or $q \not\equiv 1 \bmod p$.

Theorem 3.13.

1. $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$.
2. $g(\mathbf{q})^{p(\sigma-1)(\sigma-v)} = \pm(\frac{\overline{A}}{A})^{Q_1(\sigma)}$ *where*

$$Q_1(\sigma) = (1-\sigma) \times (\sum_{i=0}^{(p-3)/2} \delta_i \times \sigma^i) + (1-v) \times \sigma^{(p-1)/2}.$$

Proof.

1. We start of $g(\mathbf{q})^{p^2} \times \eta = A^{P(\sigma)}$ proved. Then $g(\mathbf{q})^{p^2(\sigma-1)(\sigma-v)} \times \eta^{(\sigma-1)(\sigma-v)} = A^{P(\sigma)(\sigma-1)(\sigma-v)}$. From lemma 3.11, we get

$$P(\sigma) \times (\sigma - v) \times (\sigma - 1) = p \times Q_1(\sigma) \times (\sigma^{(p-1)/2} - 1),$$

where

$$Q_1(\sigma) = (1-\sigma) \times (\sum_{i=0}^{(p-3)/2} \delta_i \times \sigma^i) + (1-v) \times \sigma^{(p-1)/2}.$$

Therefore

$$g(\mathbf{q})^{p^2(\sigma-1)(\sigma-v)} \times \eta^{(\sigma-1)(\sigma-v)} = (\frac{\overline{A}}{A})^{pQ_1(\sigma)}, \tag{19}$$

and by conjugation

$$\overline{g(\mathbf{q})}^{p^2(\sigma-1)(\sigma-v)} \times \eta^{(\sigma-1)(\sigma-v)} = (\frac{A}{\overline{A}})^{pQ_1(\sigma)}.$$

Multiplying these two relations we get, observing that $g(\mathbf{q}) \times \overline{g(\mathbf{q})} = q^f$,

$$q^{fp^2(\sigma-1)(\sigma-v)} \times \eta^{2(\sigma-1)(\sigma-v)} = 1,$$

also

$$\eta^{2(\sigma-1)(\sigma-v)} = 1,$$

and thus $\eta = \pm 1$ because $\eta \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$, which, with relation (19), leads to $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$ and achieves the proof of the first part.

2. From relation (19) we get

$$g(\mathbf{q})^{p^2(\sigma-1)(\sigma-v)} = \pm(\frac{\overline{A}}{A})^{pQ_1(\sigma)}, \tag{20}$$

so

$$g(\mathbf{q})^{p(\sigma-1)(\sigma-v)} = \pm\zeta_p^w \times (\frac{\overline{A}}{A})^{Q_1(\sigma)}, \tag{21}$$

where w is a natural number. But $g(\mathbf{q})^{\sigma-v} \in K_p$ and so $g(\mathbf{q})^{p(\sigma-v)(\sigma-1)} \in (K_p)^p$, see for instance Ribenboim [9] (2A) b. p. 118. and $(\frac{\overline{A}}{A})^{Q_1(\sigma)} \in (K_p)^p$ because $\sigma-\mu \mid Q_1(\sigma)$ in $\mathbf{F}_p[G_p]$ imply that $w = 0$, which achieves the proof of the second part.

□

Remarks

1. Observe that this theorem is true either $q \equiv 1 \bmod p$ or $q \not\equiv 1 \bmod p$.
2. $g(\mathbf{q}) \equiv -1 \bmod \pi$ implies that $g(\mathbf{q})^{p^2} \equiv -1 \bmod \pi$. Observe that if $A \equiv a \bmod \pi$ with a natural number then $A^{P(\sigma)} \equiv a^{1+v^{-1}+\cdots+v^{-(p-2)}} = a^{p(p-1)/2} \bmod \pi \equiv \pm 1 \bmod \pi$ consistent with previous result.

Lemma 3.14. *Let $q \neq p$ be an odd prime. Let f be the smallest integer such that $q^f \equiv 1$ mod p. If f is even then $g(\mathbf{q}) = \pm\zeta_p^w \times q^{f/2}$ for w a natural number.*

Proof.

1. Let $\mathbf{q}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ lying over q. From f even we get $\mathbf{q} = \overline{\mathbf{q}}$. As in first section there exists singular numbers A such that $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$.
2. From $\mathbf{q} = \overline{\mathbf{q}}$ we can choose $A \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and so $A = \overline{A}$.
3. we have $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$. From lemma 3.2 p. 6, we know that $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.
4. By complex conjugation $\overline{g(\mathbf{q})^{p^2}} = \pm A^{P(\sigma)}$. Then $g(\mathbf{q})^{p^2} = \overline{g(\mathbf{q})}^{p^2}$.
5. Therefore $g(\mathbf{q})^p = \zeta_p^{w_2} \times \overline{g(\mathbf{q})}^p$ with w_2 natural number. As $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ this implies that $w_2 = 0$ and so $g(\mathbf{q})^p = \overline{g(\mathbf{q})}^p$. Therefore $g(\mathbf{q}) = \zeta_p^{w_3} \times \overline{g(\mathbf{q})}$ with w_3 natural number. But $g(\mathbf{q}) \times \overline{g(\mathbf{q})} = q^f$ results of properties of power residue Gauss sums, see for instance Mollin prop 5.88 (b) p. 308. Therefore $g(\mathbf{q})^2 = \zeta_p^{w_3} \times q^f$ and so $(g(\mathbf{q}) \times \zeta_p^{-w_3/2})^2 = q^f$ and thus $g(\mathbf{q}) \times \zeta_p^{-w_3/2} = \pm q^{f/2}$ wich achieves the proof.

□

Theorem 3.15.

1. *If $q \equiv 1$ mod p then $A^{P(\sigma)} \equiv \delta$ mod π^{2p-1} with $\delta \in \{-1, 1\}$.*

2. *If and only if* $q \equiv 1 \ mod\ p$ *and* $p^{(q-1)/p} \equiv 1 \ mod\ q$ *then* $\pi^{2p-1} \parallel A^{P(\sigma)} - \delta$ *with* $\delta \in \{-1, 1\}$.
3. *If* $q \not\equiv 1 \ mod\ p$ *then* $A^{P(\sigma)} \equiv \delta \ mod\ \pi^{2p}$ *with* $\delta \in \{-1, 1\}$.

Proof.

1. From lemma 3.7, we get $\pi^p \mid g(\mathbf{q})^p + 1$ and so $\pi^{2p-1} \mid g(\mathbf{q})^{p^2} + 1$. Then apply theorem 3.13.
2. Applying lemma 3.8 we get $\pi^p \parallel g(\mathbf{q})^p + 1$ and so $\pi^{2p-1} \parallel g(\mathbf{q})^{p^2} + 1$. Then apply theorem 3.13.
3. From lemma 3.2, then $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ and so $\pi^{p+1} \mid g(\mathbf{q})^p + 1$ and also $\pi^{2p} \mid g(\mathbf{q})^{p^2} + 1$.

□

Remark: If $C \in \mathbb{Z}[\zeta_p]$ is any semi-primary number with $C \equiv c \bmod \pi^2$ with c natural number we can only assert in general that $C^{P(\sigma)} \equiv \pm 1 \bmod \pi^{p-1}$. For the singular numbers A considered here we assert more: $A^{P(\sigma)} \equiv \pm 1 \bmod \pi^{2p-1}$. We shall use this π-adic improvement in the sequel.

4 Polynomial congruences mod p connected to the p-class group C_p

We deal of explicit polynomial congruences connected to the p-class group when p not divides the class number h^+ of K_p^+.

1. We know that the relative p-class group $C_p^- = \oplus_{k=1}^{r^-} \Gamma_k$ where Γ_k are groups of order p annihilated by $\sigma - \mu_k$, $\mu_k \equiv v^{2m_k+1} \bmod p$, $1 \leq m_k \leq \frac{p-3}{2}$. Let us consider the singular numbers A_k, $k = 1, \ldots, r^-$, with $\pi^{2m_k+1} \mid A_k - \alpha_k$ with α_k natural numbers. From Kummer, the group of ideal classes of K_p is generated by the classes of prime ideals of degree 1 (see for instance Ribenboim [9] (3A) p. 119).
2. In this section we shall explicit a connection between the polynomial $Q(\sigma) \in \mathbb{Z}[G_p]$ and the structure of the relative p-class group C_p^- of K_p.
3. As another example we shall give an elementary proof in a straightforward way that if $\frac{p-1}{2}$ is odd then the Bernoulli Number $B_{(p+1)/2} \not\equiv 0 \bmod p$.

Theorem 4.1. *Let p be an odd prime. Let v be a primitive root mod p. For $k = 1, \ldots, r^-$ rank of the p-class group of K_p then*

$$Q(v^{2m_k+1}) = \sum_{i=1}^{p-2} v^{(2m_k+1)\times i} \times (\frac{v^{-(i-1)} - v^{-i} \times v}{p}) \equiv 0 \ mod\ p, \tag{22}$$

(or an other formulation $\prod_{k=1}^{r^-}(\sigma - v^{2m_k+1})$ divides $Q(\sigma)$ in $\mathbf{F}_p[G_p]$).

Proof.

1. Let us fix A for one the singular numbers A_k with $\pi^{2m+1} \parallel A-\alpha$ with α natural number equivalent to $\pi^{2m+1} \parallel (\frac{A}{\overline{A}} - 1)$, equivalent to

$$\frac{A}{\overline{A}} = 1 + \lambda^{2m+1} \times a, \quad a \in K_p, \quad v_\pi(a) = 0.$$

   Then raising to p-power we get $(\frac{A}{\overline{A}})^p = (1+\lambda^{2m+1}\times a)^p \equiv 1+p\lambda^{2m+1}a \bmod \pi^{p-1+2m+2}$ and so $\pi^{p-1+2m+1} \parallel (\frac{A}{\overline{A}})^p - 1$.

2. From theorem 3.15 we get

$$(\frac{A}{\overline{A}})^{P(\sigma)\times(\sigma-v)} = (\frac{A}{\overline{A}})^{pQ(\sigma)} \equiv 1 \bmod \pi^{2p-1}.$$

   We have shown that

$$(\frac{A}{\overline{A}})^p = 1 + \lambda^{p-1+2m+1}b, \quad b \in K_p, \quad v_\pi(b) = 0,$$

   then

$$(1 + \lambda^{p-1+2m+1}b)^{Q(\sigma)} \equiv 1 \bmod \pi^{2p-1}. \tag{23}$$

3. But $1+\lambda^{p-1+2m+1}b \equiv 1+p\lambda^{2m+1}b_1 \bmod \pi^{p-1+2m+2}$ with $b_1 \in \mathbb{Z}, \quad b_1 \not\equiv 0 \bmod p$. There exists a natural integer n not divisible by p such that

$$(1 + p\lambda^{2m+1}b_1)^n \equiv 1 + p\lambda^{2m+1} \bmod \pi^{p-1+2m+2}.$$

   Therefore

$$(1 + p\lambda^{2m+1}b_1)^{nQ(\sigma)} \equiv (1 + p\lambda^{2m+1})^{Q(\sigma)} \equiv 1 \bmod \pi^{p-1+2m+2}. \tag{24}$$

4. Show that the possibility of climbing up the step $\bmod \pi^{p-1+2m+2}$ implies that $\sigma - v^{2m+1}$ divides $Q(\sigma)$ in $\mathbf{F}_p[G_p]$: we have $(1 + p\lambda^{2m+1})^\sigma = 1 + p\sigma(\lambda^{2m+1}) = 1+p(\zeta^v-1)^{2m+1} = 1+p((\lambda+1)^v-1)^{2m+1} \equiv 1+pv^{2m+1}\lambda^{2m+1} \bmod \pi^{p-1+2m+2}$. In an other part $(1+p\lambda^{2m+1})^{v^{2m+1}} \equiv 1+pv^{2m+1}\lambda^{2m+1} \bmod \pi^{p-1+2m+2}$. Therefore

$$(1 + p\lambda^{2m+1})^{\sigma-v^{2m+1}} \equiv 1 \bmod \pi^{p-1+2m+2}. \tag{25}$$

5. By euclidean division of $Q(\sigma)$ by $\sigma - v^{2m+1}$ in $\mathbf{F}_p[G_p]$, we get

$$Q(\sigma) = (\sigma - v^{2m+1})Q_1(\sigma) + R$$

with $R \in \mathbf{F}_p$. From congruence (24) and (25) it follows that $(1 + p\lambda^{2m+1})^R \equiv 1 \bmod \pi^{p-1+2m+2}$ and so that $1+pR\lambda^{2m+1} \equiv 1 \bmod \pi^{p-1+2m+2}$ and finally that $R = 0$. Then in $\mathbf{F}_p$ we have $Q(\sigma) = (\sigma - v^{2m+1}) \times Q_1(\sigma)$ and so $Q(v^{2m+1}) \equiv 0 \bmod p$, or explicitly

$$Q(v^{2m+1}) = v^{(2m+1)(p-2)} \times \frac{v^{-(p-3)} - v^{-(p-2)}v}{p}$$
$$+ v^{(2m+1)(p-3)} \times \frac{v^{-(p-4)} - v^{-(p-3)}v}{p} + \cdots + v^{2m+1} \times \frac{1 - v^{-1}v}{p} \equiv 0 \bmod p,$$

which achieves the proof.

□

Remarks:

1. Observe that it is the π-adic theorem 3.15 connected to Kummer-Stickelberger which allows to obtain this result.
2. It can be shown that $g(\mathbf{q})^{\sigma - v} \in K_p$, see for instance Ribenboim [10] F. p. 440 : from this result applied to Stickelberger relation, it is possible to give another proof of theorem 4.1: we start of $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^{P(\sigma)}$ and so $g(\mathbf{q})^{p(\sigma-v)}\mathbb{Z}[\zeta_p] = \mathbf{q}^{P(\sigma)(\sigma-v)} = \mathbf{q}^{pQ(\sigma)}$ and thus $g(\mathbf{q})^{(\sigma-v)}\mathbb{Z}[\zeta_p] = \mathbf{q}^{Q(\sigma)}$. Therefore $Q(\sigma)$ annihilates the ideal class $Cl(\mathbf{q})$ and so there exists $\mu \in \mathbf{F}_p^*$ such that $\sigma - \mu \mid Q(\sigma)$ in $\mathbf{F}_p[G_p]$.
3. Observe that δ_i can also be written in the form $\delta_i = -[\frac{v^{-i} \times v}{p}]$ where $[x]$ is the integer part of x, similar form also known in the literature.
4. Observe that it is possible to get other polynomials of $\mathbb{Z}[G_p]$ annihilating the relative p-class group C_p^-: for instance from Kummer's formula on Jacobi cyclotomic functions we induce other polynomials $Q_d(\sigma)$ annihilating the relative p-class group C_p^- of K_p : If $1 \leq d \leq p-2$ define the set

$$I_d = \{i \mid 0 \leq i \leq p-2, \quad v^{(p-1)/2-i} + v^{(p-1)/2-i+ind_v(d)} > p\}$$

where $ind_v(d)$ is the minimal integer s such that $d \equiv v^s \bmod p$. Then the polynomials $Q_d(\sigma) = \sum_{i \in I_d} \sigma^i$ for $d = 1, \ldots, p-2$ annihilate the p-class C_p of K_p, see for instance Ribenboim [9] relations (2.4) and (2.5) p. 119.
5. See also in a more general context Washington, [11] corollary 10.15 p. 198.

6. It is easy to verify the consistency of relation (22) with the table of irregular primes and Bernoulli numbers in Washington, [11] p. 410.

An immediate consequence is an explicit criterium for p to be a regular prime:

Corollary 4.2. *Let p be an odd prime. Let v be a primitive root mod p. If the congruence*

$$\sum_{i=1}^{p-2} X^{i-1} \times (\frac{v^{-(i-1)} - v^{-i} \times v}{p}) \equiv 0 \ mod\ p \tag{26}$$

has no solution X in $\mathbb{Z}$ with $X^{(p-1)/2} + 1 \equiv 0$ mod p then the prime p is regular.

We give as another example a straightforward proof of following lemma on Bernoulli Numbers (compare elementary nature of this proof with proof hinted by Washington in exercise 5.9 p. 85 using Siegel-Brauer theorem).

Lemma 4.3. *If $2m+1 = \frac{p-1}{2}$ is odd then the Bernoulli Number $B_{(p+1)/2} \not\equiv 0$ mod p.*

Proof. From previous corollary it follows that if $B_{(p+1)/2} \equiv 0 \mod p$ implies that $\sum_{i=1}^{p-2} v^{(2m+1)i} \times \delta^i \equiv 0 \mod p$ where $2m+1 = \frac{p-1}{2}$ because $v^{(p-1)/2} \equiv -1 \mod p$. Then suppose that

$$\sum_{i=1}^{p-2} (-1)^i \times (\frac{v^{-(i-1)} - v^{-i} \times v}{p}) \equiv 0 \mod p,$$

and search for a contradiction: multiplying by p

$$\sum_{i=1}^{p-2} (-1)^i \times (v^{-(i-1)} - v^{-i} \times v) \equiv 0 \mod p^2,$$

expanded to

$$(-1 + v^{-1} - v^{-2} + \cdots - v^{-(p-3)}) + (v^{-1}v - v^{-2}v + \cdots + v^{-(p-2)}v) \equiv 0 \mod p^2$$

also

$$(-1 + v^{-1} - v^{-2} + \cdots - v^{-(p-3)}) + (v^{-1} - v^{-2} + \cdots + v^{-(p-2)})v \equiv 0 \mod p^2.$$

Let us set $V = -1 + v^{-1} - v^{-2} + \cdots - v^{-(p-3)} + v^{-(p-2)}$. Then we get $V - v^{-(p-2)} + v(V+1) \equiv 0 \mod p^2$, and so $V(1+v) + v - v^{-(p-2)} \equiv 0 \mod p^2$. But $v = v^{-(p-2)}$ and so $V \equiv 0 \mod p^2$. But

$$\begin{aligned} -V &= 1 - v^{-1} + v^{-2} + \cdots + v^{-(p-3)} - v^{-(p-2)} = S_1 - S_2 \\ S_1 &= 1 + v^{-2} + \cdots + v^{-(p-3)}, \\ S_2 &= v^{-1} + v^{-3} + \cdots + v^{-(p-2)}. \end{aligned}$$

v^{-1} is a primitive root mod p and so $S_1 + S_2 = \frac{p(p-1)}{2}$. Clearly $S_1 \neq S_2$ because $\frac{p(p-1)}{2}$ is odd and so $-V = S_1 - S_2 \neq 0$ and $-V \equiv 0 \bmod p^2$ with $|-V| < \frac{p(p-1)}{2}$, contradiction which achieves the proof. □

5 Singular primary numbers and Stickelberger relation

In this section we give some π-adic properties of singular numbers A when they are primary. Recall that r, r^+, r^- are the ranks of the p-class groups C_p, C_p^-, C_p^+. Recall that $C_p = \oplus_{i=1}^{r} \Gamma_i$ where Γ_i are cyclic group of order p annihilated by $\sigma - \mu_i$ with $\mu_i \in \mathbf{F}_p^*$.

5.1 The case of C_p^-

A classical result on structure of p-class group is that the relative p-class group C_p^- is a direct sum $C_p^- = (\oplus_{i=1}^{r^+} \Gamma_i) \oplus (\oplus_{i=r^++1}^{r^-} \Gamma_i)$ where the subgroups $\Gamma_i, \quad i = 1, \ldots, r^+$ correspond to *singular primary* numbers A_i and where the subgroups $\Gamma_i, \quad i = r^+ + 1, \ldots, r^-$ corresponds to *singular not primary* numbers A_i. Let us fix one of these singular primary numbers A_i for $i = 1, \ldots, r^+$. Let $\mathbf{q}$ be a prime ideal of inertial degree f such that $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$.

Theorem 5.1. *Let $\mathbf{q}$ be a prime not principal ideal of $\mathbb{Z}[\zeta_p]$ of inertial degree f with $Cl(\mathbf{q}) \in \Gamma \subset C_p^-$. Suppose that the prime number q above $\mathbf{q}$ verifies $p \parallel q^f - 1$ and that A is a singular primary number with $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$. Then*

$$A \not\equiv 1 \bmod \pi^{2p-1}. \tag{27}$$

Proof.

1. We start of the relation $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$ proved in theorem 3.13. By conjugation we get $\overline{g(\mathbf{q})}^{p^2} = \pm \overline{A}^{P(\sigma)}$. Multiplying these two relations and observing that $g(\mathbf{q}) \times \overline{g(\mathbf{q})} = q^f$ and $A \times \overline{A} = D^p$ with $D \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ we get $q^{fp^2} = D^{pP(\sigma)}$, so $q^{fp} = D^{P(\sigma)}$ because $q, D \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and, multiplying the exponent by $\sigma - v$, we get $q^{fp(\sigma - v)} = D^{P(\sigma)(\sigma - v)}$ so $q^{fp(1-v)} = D^{pQ(\sigma)}$ from lemma 3.10 p. 10 and thus

$$q^{f(1-v)} = D^{Q(\sigma)}. \tag{28}$$

2. Suppose that $\pi^{2p-1} \mid A - 1$. Then $\pi^{2p-1} \mid \overline{A} - 1$, so $\pi^{2p-1} \mid D^p - 1$ and so $\pi^p \mid D - 1$ and so $\pi^p \mid D^{Q(\sigma)} - 1$, thus $\pi^p \mid q^{f(1-v)} - 1$ and finally $\pi^p \mid q^f - 1$, contradiction with $\pi^{p-1} \parallel q^f - 1$.

□

In the following theorem we obtain a result of same nature which can be applied generally to a wider range of singular primary numbers A if we assume simultaneously the two hypotheses $q \equiv 1 \bmod p$ and $p^{(q-1)/p} \equiv 1 \bmod q$.

Theorem 5.2. *Let* $\mathbf{q}$ *be a prime not principal ideal of* $\mathbb{Z}[\zeta_p]$ *of inertial degree* $f = 1$ *with* $Cl(\mathbf{q}) \in \Gamma \subset C_p$. *Let* A *be a singular primary number with* $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$. *If* $p^{(q-1)/p} \equiv 1$ *mod* q *then there exists no natural integer* a *such that*

$$A \equiv a^p \ mod\ \pi^{2p}. \tag{29}$$

Proof. Suppose that $A \equiv a^p \bmod \pi^{2p}$ and search for a contradiction. We start of relation $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$ proved in theorem 3.13 p. 13. Therefore $g(\mathbf{q})^{p^2} \equiv \pm a^{pP(\sigma)} \bmod \pi^{2p}$, so

$$g(\mathbf{q})^{p^2} \equiv \pm a^{p(v^{-(p-2)}+\cdots+v^{-1}+1)} \bmod \pi^{2p},$$

so

$$g(\mathbf{q})^{p^2} \equiv \pm a^{p^2(p-1)/2} \bmod \pi^{2p}.$$

But $a^{p^2(p-1)/2} \equiv \pm 1 \bmod \pi^{2p}$. It should imply that $g(\mathbf{q})^{p^2} \equiv \pm 1 \bmod \pi^{2p}$, so that $g(\mathbf{q})^p \equiv \pm 1 \bmod \pi^{p+1}$ which contradicts lemma 3.8 p. 9. □

5.2 On the π-adic size of singular primary numbers

In this subsection we suppose that the p-class group C_p of rank r is not trivial. Then $C_p = \oplus_{i=1}^{r} \Gamma_i$ where Γ_i are cyclic groups of order p annihilated by $\sigma - \mu_i \in \mathbf{F}_p^*$. Let us consider in the sequel one ot these groups $\Gamma \in C_p$. From Kummer (see for instance Ribenboim [10] prop. U p. 454), the prime ideals $\mathbf{q}$ of K_p of inertial degree $f = 1$ with $N_{K_p/\mathbb{Q}}(\mathbf{q}) = q \neq p$ generate the class group of K_p. Therefore there exists prime not principal ideals $\mathbf{q}$ of inertial degree $f = 1$ with $Cl(\mathbf{q}) \in \Gamma$. Let us consider in this section a singular number $A \in \mathbb{Z}[\zeta_p]$ with $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$. There exists a natural integer $m(A)$ no null and a natural integer a no null such that $\pi^{m(A)} \parallel A - a^p$ and such that $\pi^{m(A)+1} \not| A - a'^p$ for all $a' \in \mathbb{Z}$. If A is singular not primary then $1 < m < p-1$. If A is singular primary then $m \geq p$. We call $m(A)$ the *π-adic size of A.* Recall that the Stickelberger's relation is $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = A^{P(\sigma)}$ where

$$g(\mathbf{q}) = \sum_{i=0}^{q-2} \zeta_p^{-iv} \times \zeta_q^{u^{-i}}.$$

In this subsection A is a primary number. Recall that such singular primary integers A (which are therefore not of form $\varepsilon \times a^p$, $\varepsilon \in \mathbb{Z}[\zeta_p]^*$ and $a \in \mathbb{Z}[\zeta_p]$) exist only if the Vandiver's conjecture is false ($r^+ > 0$).

Lemma 5.3. *If A is singular primary then the size $m(A)$ verifies $m \geq p+1$.*

Proof. From Washington [11] exercise 9.3 p. 183 it follows that $L = K_p(A^{1/p})/K_p$ is a cyclic unramified extension. Therefore π splits in extension L/K_p and from Ribenboim [9] case III p. 168 it follows that $\pi^{p+1} \mid A - a^p$. □

Lemma 5.4. *Let A be a singular primary number of size $m = p-1+n$. Then $\Delta(g(\mathbf{q})) = \sigma(g(\mathbf{q})) - (-1)^{v-1} g(\mathbf{q})^v \equiv 0 \ mod\ \pi^n$.*

Proof. The proof consists of the two cases $Cl(\mathbf{q}) \in C_p^+$ and $Cl(\mathbf{q}) \in C_p^-$.

1. Suppose at first that $Cl(\mathbf{q}) \in C_p^+$:

   (a) From theorem 3.13 p. 13, $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$ and $\overline{g(\mathbf{q})}^{p^2} = \pm \overline{A}^{P(\sigma)}$, so $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} = (\frac{A}{\overline{A}})^{P(\sigma)}$, thus $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} = D^{pP(\sigma)}$.

   (b) Eliminating p-powers we get $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p} = \zeta_p^w \times D^{P(\sigma)}$ for some natural number w and so $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p(\sigma-v)} = \zeta_p^{w(\sigma-v)} \times D^{P(\sigma)(\sigma-v)}$ and, from lemma 3.10 p. 10, $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p(\sigma-v)} = D^{pQ(\sigma)}$. Then, from lemma 3.11, multiplying exponent by $\sigma - 1$, we obtain $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p(\sigma-v)(\sigma-1)} = D^{pQ_1(\sigma)(\sigma^{(p-1)/2}-1)}$. From $D^{p\sigma^{(p-1)/2}} = D^{-p}$ we get

   $$(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p(\sigma-v)(\sigma-1)} = D^{-2pQ_1(\sigma)}. \tag{30}$$

   The relation $g(\mathbf{q}) \times \overline{g(\mathbf{q})} = q$ derived of Stickelberger relation leads to

   $$g(\mathbf{q})^{2p(\sigma-v)(\sigma-1)} = D^{-2pQ_1(\sigma)}. \tag{31}$$

   (c) $\pi^{p-1+n} \parallel A - a^p$ for some natural a, so $\pi^{p-1+n} \mid D^p - 1$, which implies that $\pi^{p-1+n} \mid D^{-pQ_1(\sigma)} - 1$, thus

   $$g(\mathbf{q})^{p(\sigma-v)(\sigma-1)} \equiv 1 \bmod \pi^{p-1+n}, \quad n \geq 2. \tag{32}$$

   Recall that, from lemma 3.4 p. 7 and 3.6 p. 8 that

   $$g(\mathbf{q}) = \zeta_q + \zeta_p^{-v}\zeta_q^{u^{-1}} + \zeta_p^{-2v}\zeta_q^{u^{-2}} + \cdots + \zeta_p^{-(q-2)v}\zeta_q^{u^{-(q-2)}}, \tag{33}$$

   thus $g(\mathbf{q})+1 = (\zeta_p^{-v}-1)\zeta_q^{u^{-1}} + (\zeta_p^{-2v}-1)\zeta_q^{u^{-2}} + \cdots + (\zeta_p^{-(q-2)v}-1)\zeta_q^{u^{-(q-2)}}$ which implies that $\pi \mid g(\mathbf{q})+1$. Moreover

   $$g(\mathbf{q})+1 = \lambda \times (\frac{\zeta_p^{-v}-1}{\zeta_p - 1} \times \zeta_q^{u^{-1}} + \frac{\zeta_p^{-2v}-1}{\zeta_p-1} \times \zeta_q^{u^{-2}}, + \cdots + \frac{\zeta_p^{-(q-2)v}-1}{\zeta_p-1}) \times \zeta_q^{u^{-(q-2)}}).$$

and so $g(\mathbf{q})+1 \equiv -\lambda \times (v\zeta_q^{u^{-1}} + 2v\zeta_q^{u^{-2}} + \cdots + (q-2)v\zeta_q^{u^{-(q-2)}}) \bmod \pi^2$, thus $g(\mathbf{q}) \equiv -1 + \lambda a \bmod \pi^2$ with $a \in K_q$. But $\sigma(\lambda) = \zeta^v - 1 \equiv v\lambda \bmod \pi^2$ so $\sigma(g(\mathbf{q})) \equiv -1 + av\lambda \bmod \pi^2$. But $g(\mathbf{q})^v \equiv (-1+a\lambda)^v \equiv (-1)^v + (-1)^{v-1}v\lambda \bmod \pi^2$, so $(-1)^{v-1}g(\mathbf{q})^v \equiv -1 + av\lambda \bmod \pi^2$ and thus

$$g(\mathbf{q})^{\sigma-v} \equiv (-1)^{v-1} \bmod \pi^2. \tag{34}$$

It follows that

$$g(\mathbf{q})^{(\sigma-v)(\sigma-1)} \equiv 1 \bmod \pi^2. \tag{35}$$

(d) Then, from congruence (32), (34) and (35)

$$g(\mathbf{q})^{\sigma} \equiv (-1)^{v-1} g(\mathbf{q})^v \bmod \pi^n. \tag{36}$$

2. Suppose now that $Cl(\mathbf{q}) \in C_p^-$:

(a) From theorem 3.13 p. 13 we get $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$, so $\overline{g(\mathbf{q})^{p^2}} = \pm \overline{A}^{P(\sigma)}$ and so $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} = (\frac{A}{\overline{A}})^{P(\sigma)}$, then multiplying exponent by $\sigma - v$, $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2(\sigma-v)} = (\frac{A}{\overline{A}})^{P(\sigma)(\sigma-v)}$, and from lemma 3.10 p. 10

$$(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2(\sigma-v)} = (\frac{A}{\overline{A}})^{pQ(\sigma)}, \tag{37}$$

and so $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p(\sigma-v)} = (\frac{A}{\overline{A}})^{Q(\sigma)}$. But $Q(\sigma) = Q_2(\sigma) \times (\sigma - \mu)$ where $Q_2(\sigma) \in \mathbf{F}_p[G_p]$, so $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p(\sigma-v)} = (\frac{A}{\overline{A}})^{(\sigma-\mu)Q_2(\sigma)}$.

(b) But $\pi^{p-1+n} \parallel A - a^p$ for some natural integer a. Then $\sigma(A)) \equiv a^p \bmod \pi^{p-1+n}$ and $A^\mu \equiv a^{p\mu} \bmod \pi^{(p-1)+n}$. Therefore $A^{\sigma-\mu} \equiv a^{(1-\mu)p} \bmod \pi^{p-1+n}$. From $A^{\sigma-\mu} = \alpha^p$ with $\alpha \in K_p$, we get $\alpha \equiv \zeta_p^{w_1} \times a^{1-\mu} \bmod \pi^n$ for some natural number w_1 and so $\frac{\alpha}{\overline{\alpha}} \equiv \zeta_p^{2w_1} \bmod \pi^n$.

(c) From relation (37) we get $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p(\sigma-v)} = (\frac{\alpha}{\overline{\alpha}})^{pQ_2(\sigma)}$, so $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{(\sigma-v)} = \zeta^{w_2} \times (\frac{\alpha}{\overline{\alpha}})^{Q_2(\sigma)}$ for some natural integer w_2. But $\alpha^p = A^{\sigma-\mu}$ implies that $\pi^{p-1+n} \parallel A - a^p$ and so $\pi^{p-1+n} \mid \frac{\alpha^p}{\overline{\alpha^p}} - 1$, so $\pi^n \mid \frac{\alpha}{\overline{\alpha}} - 1$. also $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{(\sigma-v)} \equiv \zeta^{w_2} \bmod \pi^n$. But $g(q)\overline{g(\mathbf{q})} = q$ so $g(\mathbf{q})^{2(\sigma-v)} \equiv \zeta^{w_2} \bmod \pi^n$, so $g(\mathbf{q})^{\sigma-v} \equiv \pm\zeta^{w_2} \bmod \pi^n$. From $g(\mathbf{q}) \equiv -1 + a\lambda \bmod \pi^2$ it follows that $g(\mathbf{q})^{(\sigma-v)} \equiv (-1)^{v-1} \bmod \pi^n$, wich achieves the proof.

□

Remark: $\Delta(g(\mathbf{q})) = (\sum_{i=0}^{q-2} \zeta_p^{-iv^2}\zeta_q^{u^{-i}}) - (-1)^{v-1}(\sum_{i=0}^{p-2} \zeta_p^{-iv}\zeta_q^{u^{-i}})^v \in \mathbb{Z}[\zeta_p, \zeta_q]$ is explicitly computable for pairs of prime number (p, q) with $q \equiv 1 \bmod p$, for instance with a MAPLE program. We have computed $\Delta(g(\mathbf{q}))$ for a large number of pairs (p, q) with small q, $p \neq 3$, $q \not\equiv 1 \bmod 3$ and we have found that for almost all these pairs $\pi^3 \parallel \Delta(g(\mathbf{q}))$ (for $p = 5$ and $q = 11$ then $\pi^4 \mid \Delta(g(\mathbf{q}))$.

1. From this result it is not unreasonable to think that if Vandiver's conjecture was false then A should be primary and the size $m(A)$ of singular primary number A should verify *often*, following these computations, the inequality $m(A) = p - 1 + n \leq p - 1 + 3$.
2. Observe that by opposite if $\varepsilon \in \mathbb{Z}[\zeta_p]^*$ is a primary unit with $\varepsilon^{\sigma-\mu} = \eta^p$, $\eta \in \mathbb{Z}[\zeta_p]$, $\mu \equiv v^{2l} \bmod p$ for some natural integer l, $1 \leq l \leq \frac{p-3}{2}$, then from Denes, as cited in Ribenboim [9] (8D) p. 192, we know that the π-adic size m of primary unit ε is of form $m(\varepsilon) = \nu \times (p-1) + 2l$ where $\nu > 0$ is a natural integer. In that case l is not always small by comparison with p.

The Jacobi cyclotomic function: It is also possible to derive some strong properties of π-adic structure of singular primary numbers using the Jacobi cyclotomic function. Let i be an integer with $1 \leq i \leq q-2$. There exists one and only one integer s, $1 \leq s \leq q-2$ such that $i \equiv u^s \bmod q$. The number s is called the *index* of i *relative* to u and denoted $s = ind_u(i)$. Let a, b be natural numbers such that $ab(a+b) \not\equiv 0 \bmod p$. The Jacobi resolvents verify the relation:

$$\frac{< \zeta_p^a, \zeta_q >< \zeta_p^b, \zeta_q >}{< \zeta_p^{a+b}, \zeta_q >} = \sum_{i=1}^{q-2} \zeta_p^{a \times ind_u(i) - (a+b) \times ind_u(i+1)} \tag{38}$$

The interest of this formula for π-adic structure of singular primary numbers is that the right member $\in \mathbb{Z}[\zeta_p]$ though the Jacobi resolvents $< \zeta_p^a, \zeta_q >$, $< \zeta_p^b, \zeta_q >$ and $< \zeta_p^{a+b}, \zeta_q >$ are in $\mathbb{Z}[\zeta_p, \zeta_q]$. See for this result for instance Ribenboim [10] proposition (I) p. 442.

Theorem 5.5. *Let A be a singular primary number of size $m(A) = p - 1 + n$. Let a, b be two natural numbers such that $ab \times (a+b) \not\equiv 0$ mod p. Then the pair of odd prime numbers (p, q), $q \equiv 1$ mod p corresponding to the singular primary number A verifies the π-adic congruences:*

1. *The Jacobi cyclotomic function*

$$\psi_{a,b}(\zeta_p) = \sum_{i=1}^{q-2} \zeta_p^{a \times ind_u(i) - (a+b) \times ind_u(i+1)} \equiv -1 \ mod\ \pi^n. \tag{39}$$

2. *For* $k = 2, \ldots, n-1$

$$\sum_{i=1}^{q-2} \{a \times ind_u(i) - (a+b) \times ind_u(i+1)\}^k \equiv 0 \ mod\ p. \tag{40}$$

Proof.

1. We start of $g(\mathbf{q}) = \sum_{i=1}^{q-2} \zeta_p^{-iv} \zeta_q^{u^{-i}}$. There exists a natural number α such that $-v^{\alpha+1} \equiv a \bmod p$. Then $< \zeta_p^a, \zeta_q > = < \zeta_p^{-vv^\alpha}, \zeta_q > = \sigma^\alpha(g(\mathbf{q}))$. From lemma 5.4, $g(\mathbf{q})^{\sigma^\alpha - v^\alpha} \equiv \pm 1 \bmod \pi^n$. Similarly $< \zeta_p^b, \zeta_q > = \sigma^\beta(g(\mathbf{q}))$ and $g(\mathbf{q})^{\sigma^\beta - v^\beta} \equiv \pm 1 \bmod \pi^n$.
2. $< \zeta_p^{a+b}, \zeta_q > = < \zeta_p^{-vv^\gamma}, \zeta_q >$ with $-v^{\gamma+1} \equiv a+b \bmod p$. Then $< \zeta_p^{a+b}, \zeta_q > = \sigma^\gamma(g(\mathbf{q}))$ with $g(\mathbf{q})^{\sigma^\gamma - v^\gamma} \equiv \pm 1 \bmod \pi^n$.
3. $$\frac{< \zeta_p^a, \zeta_q >< \zeta_p^b, \zeta_q >}{< \zeta_p^{a+b}, \zeta_q >} = \frac{\sigma^\alpha(g(\mathbf{q}))\sigma^\beta(q(\mathbf{q}))}{\sigma^\gamma(g(\mathbf{q}))} \equiv \pm g(\mathbf{q})^{v^\alpha + v^\beta - v^\gamma} \bmod \pi^n,$$

   also

   $$\frac{< \zeta_p^a, \zeta_q >< \zeta_p^b, \zeta_q >}{< \zeta_p^{a+b}, \zeta_q >} \equiv \pm g(\mathbf{q})^{v^{-1} \times (v^{\alpha+1} + v^{\beta+1} - v^{\gamma+1})} \bmod \pi^n.$$

   But $v^{\alpha+1} + v^{\beta+1} - v^{\gamma+1} \equiv -a - b + a + b \equiv 0 \bmod p$ and so

   $$\frac{< \zeta_p^a, \zeta_q >< \zeta_p^b, \zeta_q >}{< \zeta_p^{a+b}, \zeta_q >} \equiv \pm 1 \bmod \pi^n,$$

   and from Jacobi cyclotomic function relation (38)

   $$\sum_{i=1}^{q-2} \zeta_p^{a \times ind_u(i) - (a+b) \times ind_u(i+1)} \equiv \pm 1 \bmod \pi^n.$$

   But we see directly , from $\zeta_p \equiv 1 \bmod p$ and $q - 2 \equiv -1 \bmod p$, that

   $$\sum_{i=1}^{q-2} \zeta_p^{a \times ind_u(i) - (a+b) \times ind_u(i+1)} \equiv -1 \bmod \pi,$$

   and finally that

   $$\sum_{i=1}^{q-2} \zeta_p^{a \times ind_u(i) - (a+b) \times ind_u(i+1)} \equiv -1 \bmod \pi^n,$$

   which proves relation (39).

4. The congruences (40) are an immediate consequence, using logarithmic derivatives.

□

This result takes a very simple form when $a = 1$ and $b = -2$.

Corollary 5.6. *Let A be a singular primary number of size $m(A) = p-1+n$. Then the pair of odd prime numbers (p, q), $q \equiv 1$ mod p corresponding to the singular primary number A verifies the π-adic congruences of the Jacobi cyclotomic function*

$$\psi_{1,-2}(\zeta_p) = \sum_{i=1}^{q-2} \zeta_p^{ind_u(i(i+1))} \equiv -1 \ mod\ \pi^n. \tag{41}$$

Proof. Take $a = 1$ and $b = -2$ in congruence (39) to get

$$\sum_{i=1}^{q-2} \zeta_p^{ind_u(i)+ind_u(i+1)} \equiv -1 \bmod \pi^n. \tag{42}$$

But classically $ind_u(i) + ind_u(i+1) \equiv ind_u(i(i+1)) \bmod (q-1)$ and so from $q \equiv 1 \bmod p$ we get $ind_u(i) + ind_u(i+1) \equiv ind_u(i(i+1)) \bmod p$ which achieves the proof. □

Remark: We have computed $\psi_{1,-2}(\zeta_p)$ for a large number of pairs (p, q) with small q, $p \neq 3$, $q \not\equiv 1 \bmod 3$ and we have found that for almost all these pairs $\pi^3 \parallel \psi_{1,-2}(\zeta_p)$.

5.3 On principal prime ideals of K_p and Stickelberger relation

The Stickelberger relation and its consequences on prime ideals $\mathbf{q}$ of $\mathbb{Z}[\zeta_p]$ is meaningful even if $\mathbf{q}$ is a principal ideal.

Theorem 5.7. *Let $q_1 \in \mathbb{Z}[\zeta_p]$ with $q_1 \equiv a$ mod π^{p+1} where $a \in \mathbb{Z}$, $a \not\equiv 0$ mod p. If $q = N_{K_p/\mathbb{Q}}(q_1)$ is a prime number then $p^{(q-1)/p} \equiv 1$ mod q.*

Proof. From Stickelberger relation $g(q_1\mathbb{Z}[\zeta_p])^p\mathbb{Z}[\zeta_p] = q_1^{P(\sigma)}\mathbb{Z}[\zeta_p]$ and so there exists $\varepsilon \in \mathbb{Z}[\zeta_p]^*$ such that $g(q_1\mathbb{Z}[\zeta_p])^p = q_1^{P(\sigma)} \times \varepsilon$ and so

$$(\frac{g(q_1\mathbb{Z}[\zeta_p])}{\overline{g(q_1\mathbb{Z}[\zeta_p]}})^p = (\frac{q_1}{\overline{q_1}})^{P(\sigma)}.$$

From hypothesis $\frac{q_1}{\overline{q_1}} \equiv 1 \bmod \pi^{p+1}$ and so $(\frac{g(q_1\mathbb{Z}[\zeta_p]}{g(q_1\mathbb{Z}[\zeta_p]})^p \equiv 1 \bmod \pi^{p+1}$. From lemma 3.8 p. 9 it follows that $p^{(q-1)/p} \equiv 1 \bmod q$. □

6 Stickelberger's relation for prime ideals q of inertial degree $f > 1$.

Recall that the Stickelberger's relation is $g(\mathbf{q})^p = \mathbf{q}^S$ where $S = \sum_{i=0}^{p-2} \sigma^i v^{-i} \in \mathbb{Z}[G_p]$. We apply Stickelberger's relation with the same method to prime ideals $\mathbf{q}$ of inertial degree $f > 1$. Observe, from lemma 3.2 p. 6, that $f > 1$ implies $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.

A definition: we say that the prime ideal $\mathbf{c}$ of a number field M is p-principal if the component of the class group $< Cl(\mathbf{c}) >$ in p-class group D_p of M is trivial.

Lemma 6.1. *Let p be an odd prime. Let v be a primitive root mod p. Let q be an odd prime with $q \neq p$. Let f be the smallest integer such that $q^f \equiv 1$ mod p and let $m = \frac{p-1}{f}$. Let $\mathbf{q}$ be an prime ideal of $\mathbb{Z}[\zeta_p]$ lying over q. If $f > 1$ then $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ and $g(\mathbf{q})\mathbb{Z}[\zeta_p] = \mathbf{q}^{S_2}$ where*

$$S_2 = \sum_{i=0}^{m-1} \left(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}\right) \times \sigma^i \in \mathbb{Z}[G_p]. \tag{43}$$

Proof.

1. Let $p = fm + 1$. Then $N_{K_p/\mathbb{Q}}(\mathbf{q}) = q^f$ and $\mathbf{q} = \mathbf{q}^{\sigma^m} = \cdots = \mathbf{q}^{\sigma^{(f-1)m}}$. The sum S defined in lemma 3.5 p.8 can be written
$$S = \sum_{i=0}^{m-1} \sum_{j=0}^{f-1} \sigma^{i+jm} v^{-(i+jm)}.$$

2. From Stickelberger's relation seen in theorem 3.1 p. 5, then $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^S$. Observe that, from hypothesis, $\mathbf{q} = \mathbf{q}^{\sigma^m} = \cdots = \mathbf{q}^{\sigma^{(f-1)m}}$ so Stickelberger's relation implies that $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^{S_1}$ with
$$S_1 = \sum_{i=0}^{m-1} \sum_{j=0}^{f-1} \sigma^i v^{-(i+jm)} = p \times \sum_{i=0}^{m-1} \left(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}\right) \times \sigma^i,$$
where $(\sum_{i=0}^{f-1} v^{-(i+jm)})/p \in \mathbb{Z}$ because $v^{-m} - 1 \not\equiv 0 \bmod p$.

3. Let $S_2 = \frac{S_1}{p}$. Then from below $S_2 \in \mathbb{Z}[G_p]$. From lemma 3.2 p. 6 we know that $f > 1$ implies that $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$. Therefore
$$g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^{pS_2}, \quad g(\mathbf{q}) \in \mathbb{Z}[\zeta_p],$$
and so
$$g(\mathbf{q})\mathbb{Z}[\zeta_p] = \mathbf{q}^{S_2}, \quad g(\mathbf{q}) \in \mathbb{Z}[\zeta_p].$$

□

Remarks

1. For $f = 2$ the value of polynomial S_2 obtained from this lemma is $S_2 = \sum_{i=1}^{(p-3)/2} \sigma^i$.
2. Let $\mathbf{q}$ be a prime not principal ideal of inertial degree $f > 1$ with $Cl(\mathbf{q}) \in C_p$. The **two** polynomials of $\mathbb{Z}[G_p]$, $S = \sum_{i=0}^{p-2} (\frac{v^{-(i-1)} - v^{-i} v}{p}) \times \sigma^i$ (see thm 4.1) and $S_2 = \sum_{i=0}^{m-1} (\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times \sigma^i$ (see lemma 6.1)annihilate the ideal class $Cl(\mathbf{q})$. When $f > 1$ the lemma 6.1 supplement the theorem 4.1

It is possible to derive some explicit congruences in $\mathbb{Z}$ from this lemma.

Lemma 6.2. *Let p be an odd prime. Let v be a primitive root mod p. Let q be an odd prime with $q \neq p$. Let f be the smallest integer such that $q^f \equiv 1$ mod p and let $m = \frac{p-1}{f}$. Let $\mathbf{q}$ be an prime ideal of $\mathbb{Z}[\zeta_p]$ lying over q. Suppose that $f > 1$.*

1. *If $\mathbf{q}$ is not p-principal ideal there exists a natural integer $l,\ 1 \leq l < m$ such that*

$$\sum_{i=0}^{m-1} (\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times v^{lfi} \equiv 0 \ mod\ p, \tag{44}$$

2. *If for all natural integers l such that $1 \leq l < m$*

$$\sum_{i=0}^{m-1} (\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times v^{lfi} \not\equiv 0 \ mod\ p, \tag{45}$$

then $\mathbf{q}$ is p-principal

Proof.

1. Suppose that $\mathbf{q}$ is not p-principal. Observe at first that congruence (44) with $l = m$ should imply that $\sum_{i=0}^{m-1} (\sum_{j=0}^{f-1} v^{-(i+jm)})/p) \equiv 0 \bmod p$ or $\sum_{i=0}^{m-1} \sum_{j=0}^{f-1} v^{-(i+jm)} \equiv 0 \bmod p^2$ which is not possible because $v^{-(i+jm)} = v^{-(i'+j'm)}$ implies that $j = j'$ and $i = i'$ and so that $\sum_{i=0}^{m-1} \sum_{j=0}^{f-1} v^{-(i+jm)} = \frac{p(p-1)}{2}$.
2. The polynomial S_2 of lemma 6.1 annihilates the not p-principal ideal $\mathbf{q}$ in $\mathbf{F}_p[G_p]$ only if there exists $\sigma - v^n$ dividing S_2 in $\mathbf{F}_p[G_p]$. From $\mathbf{q}^{\sigma^m - 1} = 1$ it follows also that $\sigma - v^n \mid \sigma^m - 1$. But $\sigma - v^n \mid \sigma^m - v^{nm}$ and so $\sigma - v^n \mid v^{nm} - 1$, thus $nm \equiv 0 \bmod p-1$, so $n \equiv 0 \bmod f$ and $n = lf$. Therefore if $\mathbf{q}$ is not p-principal there exists a natural integer $l,\ 1 \leq l < m$ such that

$$\sum_{i=0}^{m-1} (\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times v^{lfi} \equiv 0 \bmod p, \tag{46}$$

3. The relation (45) is an imediate consequence of previous part of the proof.

□

As an example we deal with the case $f = \frac{p-1}{2}$.

Corollary 6.3. *If $p \equiv 3$ mod 4 and if $f = \frac{p-1}{2}$ then $\mathbf{q}$ is p-principal.*

Proof. We have $f = \frac{p-1}{2}$, $m = 2$ and $l = 1$. Then

$$\Sigma = \sum_{i=0}^{m-1} \left(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}\right) \times v^{lfi} = \frac{\sum_{j=0}^{(p-3)/2} v^{-2j}}{p} - \frac{\sum_{j=0}^{(p-3)/2} v^{-(1+2j)}}{p}. \tag{47}$$

$\Sigma \equiv 0 \bmod p$ should imply that $\sum_{j=0}^{(p-3)/2} v^{-2j} - \sum_{j=0}^{(p-3)/2} v^{-(1+2j)} \equiv 0 \bmod p^2$. But $\sum_{j=0}^{(p-3)/2} v^{-2j} + \sum_{j=0}^{(p-3)/2} v^{-(1+2j)} = \frac{p(p-1)}{2}$ is odd, which achieves the proof. □

7 Stickelberger relation and class group of K_p

In previous sections we considered the p-class group of K_p. By opposite, in this section we apply Stickelberger relation to all the prime $h \neq p$ dividing the class number $h(K_p)$.

1. The class group $\mathbf{C}$ of K_p is the direct sum of the class group $\mathbf{C}^+$ of the maximal totally real subfield K_p^+ of K_p and of the relative class group $\mathbf{C}^-$ of K_p.
2. Remind that v is a primitive root mod p and that v^n is to be be understood as $v^n \bmod p$ with $1 \leq v^n \leq p-1$. Let $h(K_p)$ be the class number of K_p. Let $h \neq p$ be an odd prime dividing $h(K_p)$, with $v_h(h(K_p)) = \beta$. Let $d = Gcd(h-1, p-1)$. Let C be the subgroup of the class group of K_p of order h^β. Then $C = \oplus_{j=1}^{\rho} C_j$ where ρ is the h-rank of the abelian group C of order h^β and C_j are cyclic groups of order h^{β_j}.
3. From Kummer (see for instance Ribenboim [9] (3A) p. 119), the prime ideals of $\mathbb{Z}[\zeta_p]$ of inertial degree 1 generate the ideal class group. Therefore there exist prime ideal $\mathbf{q}$ of inertial degree 1 such that $< Cl(\mathbf{q}) >= \oplus_{j=1}^{\rho} c_j$ where c_j is a cyclic group of order h and so that $< Cl(\mathbf{q}) >$ is of order h^ρ.
4. Let $P(\sigma) = \sum_{k=0}^{p-2} \sigma^k v^{-k}$. From lemma 3.5 p. 8 Stickelberger relation is $\mathbf{q}^{P(\sigma)}\mathbb{Z}[\zeta_p] = g(\mathbf{q})^p\mathbb{Z}[\zeta_p]$ where $g(\mathbf{q})^p \in \mathbb{Z}[\zeta_p]$. Therefore $\mathbf{q}^{P(\sigma)}$ is principal, a fortiori is C-principal (or $Cl(\mathbf{q})^{P(\sigma)}$ has a trivial component in C). There exists a minimal polynomial $V(X) \in \mathbf{F}_h(X)$ of degree ρ such that $\mathbf{q}^{V(\sigma)}$ is C-principal. Therefore the irreducible polynomial $V(X)$ divides $P(X)$ in $\mathbf{F}_h[X]$ for the indeterminate X because $h \neq p$.

5. $N_{K_p/\mathbb{Q}}(\mathbf{q}) = \mathbf{q}^{\sum_{k=0}^{p-2}\sigma^k}$ is principal and similarly $V(X)$ divides $T(X) = \sum_{k=0}^{p-2} X^k$ in $\mathbf{F}_h[X]$.
6. If $Cl(\mathbf{q}) \in \mathbf{C}^-$ then $\mathbf{q}^{\sigma^{(p-1)/2}+1}$ is principal.
7. Let $D(X) \in \mathbf{F}_h(X)$ defined by $D(X) = Gcd(P(X), T(X)) \bmod h$. Let $D^-(X) \in \mathbf{F}_h(X)$ defined by $D^-(X) = Gcd(P(X), X^{(p-1)/2} + 1) \bmod h$.

We have proved the following proposition:

Lemma 7.1. *There exists an irreducible polynomial $V(X) \in \mathbf{F}_h[X]$ of degree ρ such that $V(\sigma)$ annihilates C and $V(X)$ divides $D(X)$ in $\mathbf{F}_h[X]$.*

Lemma 7.2. *Suppose that C belongs to relative p-class group of K_p. Let $D^-(X) = Gcd(P(X), X^{(p-1)/2} + 1)$. Then $V(X)$ divides $D^-(X)$ in $\mathbf{F}_h[X]$.*

When C is cyclic we get:

Lemma 7.3. *If C is cyclic then:*

1. *$V(X) = X - \nu$ with $\nu \in \mathbf{F}_h^*$.*
2. *In $\mathbf{F}_h(X)$*

$$\begin{aligned} &V(X) \mid X^d - 1,\ d = gcd(h-1, p-1), \\ &V(X) \mid \{\sum_{i=0}^{d-1} X^i \times \sum_{k=0}^{(p-1)/d-1} v^{-(i+jd)}\}. \end{aligned} \tag{48}$$

3. *If h is an odd prime with the class number $h(E)$ of all intermediate fields $\mathbb{Q} \subset E \subset K_p,\ E \neq K_p$ then $d = p - 1$.*

Proof.

1. $\rho = 1$ implies that $V(\sigma) = \sigma - \nu$.
2. $X - \nu \mid X^{h-1} - \nu^{h-1}$ and so $\sigma^{h-1} - \nu^{h-1}$ annihilates C. From $\nu^{h-1} \equiv 1 \bmod h$ it follows that $\sigma^{h-1} - 1$ annihilates C. $\sigma^{p-1} - 1$ annihilates C and so $\sigma^d - 1$ annihilates C and so $X - \nu$ divides $X^d - 1$ in $\mathbf{F}_h[X]$. Then apply previous theorem.
3. From theorem 10.8 p. 188 on class group in Washington [11] , with $\rho = 1$ it follows that $h \equiv 1 \bmod p - 1$.

□

Lemma 7.4. *Let L be a subfield of K_p with $[L:\mathbb{Q}]=d$. Let h be an odd prime number dividing $h(L)$. Then in $\mathbf{F}_h[X]$*

$$
\begin{aligned}
&V(X) \mid \sum_{i=0}^{d-1} X^i, \\
&V(X) \mid \{\sum_{i=0}^{d-1} X^i \times \sum_{k=0}^{(p-1)/d-1} v^{-(i+jd)}\}.
\end{aligned} \tag{49}
$$

Proof. σ^d-1 annihilates C. Then the result can be derived for instance of Mollin [6] corollary 5.127 p. 322. □

Some examples: Our results are consistent with examples taken in tables of relative class numbers of $\mathbb{Q}(\zeta_n)$, $3 \leq n \leq 1020$, given in Washington [11], p. 412-420: verification made with a little MAPLE program.

1. $p=131$, $p-1=2\times 5\times 13$.
   (a) $h=3, v_h=3$, $\rho=3$, $d=2$, $V(\sigma)=\sigma^3+2\sigma^2+1$: C is not cyclic
   (b) $h=5$, $v_h=2$, $\rho=1$, $d=2$, $v=2$, $V(\sigma)=\sigma+1$: this group is cyclic. The theorem 7.3 relation(48) can be applied. Actually $\sum_{i=0}^{129}(-1)^i 2^{-i} = -5\times 131 \equiv 0 \bmod 5$. Observe that theorem 10.8 p. 187 in Washington [11] cannot be applied here because $h \mid h(\mathbb{Q}(\sqrt{-131})$.
   (c) $h=53$, $v_h=1$, $\rho=1$, $d=26$, $V(\sigma)=\sigma+46$: C is cyclic. $d\neq p-1=130$ and so there exists a field E, $\mathbb{Q}\subset E\subset K_p$ such that $h \mid h(E)$.
   (d) $h=1301$, $v_h=1$, $\rho=1$, $d=130$, $V(\sigma)=\sigma+283$: C is cyclic.
   (e) $h=4673706701$, $v_h=1$, $\rho=1$, $d=130$, $V(\sigma)=\sigma+3346914817$: cyclic.
2. (a) $p=137$, $p-1=2^3\times 17$.
   (b) $h=17$, $v_h=2$, $\rho=1$, $d=8$, $V(\sigma)=\sigma+8$: cyclic.
   (c) $h=47737$, $v_h=1$, $\rho=1$, $d=136$, $V(\sigma)=\sigma+13288$: cyclic.
   (d) $h=46890540621121$, $v_h=1$, $\rho=1$, $d=136$, $V(\sigma)=\sigma+14017446570735$: cyclic.
3. $p=167$, $p-1=2\times 83$.
   (a) $h=11$, $v_h=1$, $\rho=1$, $d=2$, $V(\sigma)=\sigma+1$. The theorem 7.3 relation(48) can be applied. Actually $\sum_{i=0}^{165}(-1)^i 2^{-i} = -11\times 167 \equiv 0 \bmod 11$. Observe that theorem 10.8 p. 187 in Washington [11] cannot be applied here because $h \mid h(\mathbb{Q}(\sqrt{-167})$.
   (b) $h=499$, $v_h=1$, $\rho=1$, $d=166$, $V(\sigma)=\sigma+491$: cyclic.
   (c) $h=5123189985484229035947419$, $\rho=1$, $d=166$,
   $V(\sigma)=\sigma+69813093775234443256279$: cyclic.

Some Remarks

1. Remind that we have assumed that h is **odd**.
2. In our propositions we apply the **simultaneous** annihilation of subgroup C of the class group by the norm polynomial $N(\sigma) = \sum_{k=0}^{p-2} \sigma^i$ and by the Stickelberger polynomial $\sum_{k=0}^{p-2} \sigma^i v^{-i}$, which improves strongly the result obtained with the only norm polynomial.
3. We obtain with our results a full description of the relative class group $\mathbf{C}^-$ of K_p in the three examples $p = 131$, $p = 137$ and $p = 167$.
4. We can say something on subgroup C even if there exists a field E, $\mathbb{Q} \subset E \subset K_p$ with $h \mid h(E)$. By opposite the hypothesis $h \not| h(E)$ for all E, $\mathbb{Q} \subset E \subset K_p$, $E \neq K_p$ is assumed in theorem 10.8 p. 187 in Washington [11].
5. Let δ be an integer $1 \leq \delta \leq p-2$. There exists an integer s, $0 \leq s \leq p-2$ such that $\delta \equiv v^s \bmod p$. s is called the index of δ relative to v and denoted $s = ind_v(\delta)$. Let us define the polynomial

$$
\begin{aligned}
& Q(X) = \sum_{i \in I_\delta} X^i, \\
& I_\delta = \{i \mid 0 \leq i \leq p-2,\ v_{(p-1)/2-i} + v_{(p-1)/2-i+ind_v(\delta)} > p\}.
\end{aligned} \tag{50}
$$

   From a result of Kummer on Jacobi cyclotomic functions, the polynomial $Q(\sigma)$ annihilates the complete class group $\mathbf{C}$ of K_p (see for instance Ribenboim [9] relation (2.5) p. 119). It follows that $V(X) \mid Q(X)$ in $\mathbf{F}_h[X]$ gives another criterium for the study of the structure of the group C.
6. The results can be generalized to the cyclotomic fields $K_n = \mathbb{Q}(\zeta_n)$ where n is not prime.

Complex quadratic fields : In this paragraph we formulate directly previous result when h divides the class number of the complex quadratic field $\mathbb{Q}(\sqrt{-p}) \subset K_p$, $p \equiv 3 \bmod 4$, $p \neq 3$.

Theorem 7.5. *Suppose that $p \equiv 3$ mod 4, $p \neq 3$. If h is an odd prime with $h \mid h(\mathbb{Q}(\sqrt{-p}))$ then*

$$
\sum_{i=0}^{p-2} (-1)^i v^{-i} \equiv 0 \ mod\ h. \tag{51}
$$

Proof. Let $\mathbf{Q}$ be the prime of $\mathbb{Q}(\sqrt{-p})$ lying above $\mathbf{q}$. $p \equiv 3 \bmod 4$ implies that $\sigma(\mathbf{Q})\mathbb{Z}[\zeta_p] = \overline{\mathbf{Q}}\mathbb{Z}[\zeta_p]$ and so $\mathbf{Q}^{\sigma+1}$ is principal. Therefore $\mathbf{Q}^{\sum_{i=0}^{p-2}(-1)^i v^{-i}}$ is principal and $\sum_{i=0}^{p-2}(-1)^i v^{-i} \equiv 0 \bmod h$. □

Remarks:

1. The theorem 7.7 can also be obtained from Hilbert Theorem 145 see Hilbert [3] p. 119. See also Mollin, [6] theorem 5.119 p. 318.
2. From lemmas 3.10 p. 10 and 3.11 p. 11 we could prove similarly:
   Suppose that $p \equiv 3 \bmod 4,\ p \neq 3$. If h is an odd prime with $h \mid h(\mathbb{Q}(\sqrt{-p}))$ then
   $$2 \times \sum_{i=0}^{(p-3)/2} (-1)^i v^{-i} - p \equiv 0 \bmod h. \tag{52}$$
3. Numerical evidences easily computable show more: If $p \neq 3$ is prime with $p \equiv 3 \bmod 4$ then the class number $h(\mathbb{Q}(\sqrt{-p})$ verifies
   $$h(\mathbb{Q}(\sqrt{-p}) = -\frac{\sum_{i=0}^{p-2}(-1)^i v^{-i}}{p}. \tag{53}$$
   This result has been proved by Dirichlet by analytical number theory, see Mollin remark 5.124 p. 321. It is easy to verify this formula in tables of class numbers of complex quadratic fields in some authors:
   (a) H. Cohen [2] p. 502- 505, all the table for $p \leq 503$.
   (b) in Wolfram table of quadratic class numbers [12] for large p.
   (c) Ramachandran in [8] for non cyclic class groups table 9 p. 16.

Theorem 7.6. *Suppose that $p \equiv 3$ mod 4, $p \neq 3$. If h is an odd prime with $h \mid h(\mathbb{Q}(\sqrt{-p}))$ then*

$$\begin{aligned} \sum_{i=0,\ v^{-i}\ odd}^{p-2} (-1)^i &\neq 0, \\ \sum_{i=0,\ v^{-i}\ odd}^{p-2} (-1)^i &\equiv 0 \ mod\ h. \end{aligned} \tag{54}$$

Proof. $\frac{p-1}{2}$ is odd. Apply Stickelberger relation to field $\mathbb{Q}(\zeta_{2p}) = \mathbb{Q}(\zeta_p)$. In that case $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i (v')^{-i}$ where $(v')^{-i} = v^{-i}$ if v^{-i} is odd and $(v')^{-i} = v^{-i} + p$ if v^{-i} is even. Then $p \times \sum_{i=0,\ v^{-i}\ \text{odd}}^{p-2} \sigma^i$ annihilates the class C. □

Theorem 7.7. *Suppose that $p \equiv 3$ mod 4, $p \neq 3$. Let δ be an integer $1 \leq \delta \leq p-2$. Let I_δ be the set*

$$I_\delta = \{i \mid 0 \leq i \leq p-2,\ v_{(p-1)/2-i} + v_{(p-1)/2-i+ind_v(\delta)} > p\}, \tag{55}$$

where, as seen above, $ind_v(\delta)$ is the notation index of δ relative to v. If h is an odd prime with $h \mid h(\mathbb{Q}(\sqrt{-p}))$ then

$$\begin{aligned} &\sum_{i\in I_\delta}(-1)^i \neq 0, \\ &\sum_{i\in I_\delta}(-1)^i \equiv 0 \ mod\ h. \end{aligned} \tag{56}$$

Proof. I_δ has an odd cardinal. Then see relation (55). □

Remark:

1. Observe that results of theorems 7.6 and 7.7 are consistent with existing tables of quadratic fields, for instance Arno, Robinson, Wheeler [1]. Numerical verifications seem to show more :

$$\sum_{i=0,\ v^{-i}\ odd}^{p-2} (-1)^i \equiv 0 \bmod h(\mathbb{Q}(\sqrt{-p}). \tag{57}$$

2. Observe that if $p \equiv 1 \bmod 4$ then $\sum_{i=0,v^{-i}\ \mathrm{odd}}^{p-2}(-1)^i = \sum_{i\in I_\delta} = 0$.

Biquadratic fields: the following example is a generalization for the biquadratic fields L which are included in p-cyclotomic field K_p with $p \equiv 1 \bmod 4$.

Theorem 7.8. *Let p be a prime with $2^2 \parallel p-1$. Let*

$$S = (\sum_{i=0}^{(p-3)/2} (-1)^i v^{2i})^2 + (\sum_{i=0}^{(p-3)/2} (-1)^i v^{2i+1})^2. \tag{58}$$

Let L be the field with $\mathbb{Q}(\sqrt{p}) \subset L \subset K_p$, $[L : \mathbb{Q}(\sqrt{p})] = 2$. Let h be an odd prime number with $h \mid h(L)$ and $h \not\mid h(Q(\sqrt{p})$. Then $S \neq 0$ and $S \equiv 0$ mod p.

Proof. $V(\sigma) \mid \sigma^4 - 1$. $h \not\mid h(\mathbb{Q}(\sqrt{p})$ and so $V(\sigma) \mid \sigma^2 + 1$. $P(\sigma) = \sum_{i=0}^{(p-3)/2} \sigma^{2i} v^{-2i} + \sigma \times \sum_{i=0}^{(p-3)/2} \sigma^{2i} v^{2i+1}$. Relation (58) follows. □

Remarks:

1. S does not depend of the primitive root $v \bmod p$ chosen.
2. Numerical computations seem to show more : $S \equiv 0 \bmod p^2$ and so

$$\frac{(\sum_{i=0}^{(p-3)/2}(-1)^i v^{2i})^2 + (\sum_{i=0}^{(p-3)/2}(-1)^i v^{2i+1})^2}{p^2} \equiv 0 \bmod h. \tag{59}$$

References

[1] S. Arno, M.L. Robinson, F.S. Wheeler *Imaginary quadratic fields with small odd class number*, Acta Arith. 83, 1998, 295-300.

[2] H. Cohen, A course in computational number theory, Springer-Verlag, 1993.

[3] D. Hilbert, *The Theory of Algebraic Numbers*, Springer, 1998

[4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1982.

[5] H. Koch, *Algebraic Number Theory*, Springer, 1997.

[6] R.A. Mollin, *Algebraic Number Theory*, Chapman and Hall/CRC, 1999.

[7] W. Narkiewicz, *Elementary and Analytic Theory of Numbers*, Springer-verlag, 1990.

[8] M.J. Jacobson, S. Ramachandran, and H.C. Williams, *Supplementary tables for numerical results on class groups of imaginary quadratic fields*
http://www. math.tu-berlin.de/ kant/Proceedings

[9] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[10] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.

[11] L.C. Washington, *Introduction to cyclotomic fields, second edition*, Springer, 1997.

[12] *Class number of quadratic fields*,
http://www. mathworld.wolfram.com/ClassNumber.html